SAFEBOOK 4

Allen-Bradley

Guardmaster®

Sicherheitsbezogene Steuerungssysteme für Maschinen

Grundsätze, Normen und Realisierung

LISTEN. THINK. SOLVE.SM

Rockwell Automation

Inhalt

Kapitel 1 **Vorschriften 2**
EU-Richtlinien und -Gesetzgebung, Maschinenrichtlinie, Arbeitsmittel-Benutzungsrichtlinie, Vorschriften in den USA, Occupational Safety and Health Administration (OSHA), Vorschriften in Kanada

Kapitel 2 **Normen 18**
ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission), harmonisierte europäische EN-Normen, US-Normen, OSHA-Normen, ANSI-Normen, kanadische Normen, australische Normen

Kapitel 3 **Sicherheitsstrategie 23**
Risikobeurteilung, Bestimmung von Maschinengrenzen, Erkennung von Aufgaben und Gefahren, Risikoabschätzung und Risikominderung, eigensichere Konstruktion, Schutzsysteme und -maßnahmen, Beurteilung, Schulung, persönliche Schutzausrüstung, Normen

Kapitel 4 **Schutzmaßnahmen und ergänzende Ausrüstung 36**
Zugriffsverhinderung, fest installierte, geschlossene Schutzvorrichtungen, Zugriffserkennung sowie Sicherheitsprodukte und -systeme

Kapitel 5 **Berechnen des Sicherheitsabstands 59**
Formeln, Anleitungen und Anwendung von Sicherheitslösungen unter Verwendung der Berechnungen für Sicherheitsabstände zur sicheren Steuerung beweglicher Teile, die möglicherweise eine Gefahr darstellen

Kapitel 6 **Verhinderung unerwarteten Einschaltens 63**
Verriegelung/Kennzeichnung nach Trennung von der Energiequelle (Lockout/Tagout), Systeme mit Sicherheitsisolierung, Lastabschaltungen, Schlüsseltransfersysteme, Alternativen zur Verriegelung

Kapitel 7 **Sicherheitsbezogene Steuerungssysteme und funktionale Sicherheit 65**
Einleitung zur funktionalen Sicherheit IEC/EN 62061 und EN ISO 13849-1:2008, SIL und IEC/EN 62061, PL und EN ISO 13849-1:2008, Vergleich von PL und SIL

Kapitel 8 **Systemaufbau gemäß EN ISO 13849-1:2008 ..... 71**
Architekturen von Sicherheitssystemen (Strukturen), Einsatzzeit, mittlere Zeit bis zu einem gefährlichen Ausfall (Mean Time to Dangerous Failure; MTTFd), Diagnosedeckungsgrad (Diagnostic Coverage; DC), Ausfälle aufgrund gemeinsamer Ursache (Common Cause Failure; CCF), systembedingter Ausfall, Performance Level (PL), Aufbau von Subsystemen und Kombinationen, Validierung, Inbetriebnahme von Maschinen, Fehlerausschluss

Kapitel 9 **Systemaufbau gemäß IEC/EN 62061 ..... 94**
Aufbau von Subsystemen – IEC/EN 62061, Auswirkung des Prüfintervalls, Auswirkung der Analyse von Ausfällen aufgrund gemeinsamer Ursache, Übergangsmethode für Kategorien, architekturbedingte Einschränkungen, B10 und $B10_d$, Ausfälle aufgrund gemeinsamer Ursache (Common Cause Failure; CCF), Diagnosedeckungsgrad (Diagnostic Coverage; DC), Hardwarefehlertoleranz, Verwaltung der funktionalen Sicherheit, Wahrscheinlichkeit eines gefährlichen Ausfalls (Probability of Dangerous Failure; PFHd), Prüfintervall, Anteil ungefährlicher Ausfälle (Safe Failure Fraction; SFF), systembedingter Ausfall

Kapitel 10 **Überlegungen zur Struktur sicherheitsbezogener Steuerungssysteme 106**
Überblick, Kategorien von Steuerungssystemen, unerkannte Fehler, Komponenten- und Systemklassifizierungen, Fehlerüberlegungen, Fehlerausschlüsse, Ausschaltkategorien gemäß IEC/EN 60204-1 und NFPA 79, Anforderungen an Sicherheitssteuerungssysteme in den USA, Roboternormen: USA und Kanada

Kapitel 11 **Anwendungsbeispiel unter Verwendung von SISTEMA 130**
Anwendungsbeispiel zu den Einsatzmöglichkeiten des Tools SISTEMA Performance Level Calculator mit der Rockwell Automation SISTEMA-Produktbibliothek

EU-Richtlinien und Gesetzgebung

Dieses Kapitel ist ein Leitfaden für jeden, der sich mit Maschinensicherheit befasst, wobei speziell auf Schutzvorrichtungen und Sicherheitssysteme in der Europäischen Union eingegangen wird. Zielgruppe sind Entwickler und Nutzer industrieller Anlagen.

Um den Gedanken eines offenen Marktes im Europäischen Wirtschaftsraum (EWR) (dieser umfasst alle EU-Mitgliedsstaaten sowie drei weitere Länder) zu fördern, sind alle Mitgliedsstaaten verpflichtet, Gesetze in Kraft zu setzen, die grundlegende Sicherheitsanforderungen für Maschinen und deren Benutzung definieren.

Maschinen, die diese Anforderungen nicht erfüllen, dürfen in die Länder oder innerhalb der Länder des EWR nicht geliefert werden.

Verschiedene europäische Richtlinien beziehen sich auf die Sicherheit von Industriemaschinen und -anlagen, doch die beiden folgenden Richtlinien sind die mit der direktesten Relevanz:

1 Maschinenrichtlinie

2 Arbeitsmittel-Benutzungsrichtlinie

Diese beiden Richtlinien stehen in direktem Zusammenhang, da die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen der Maschinenrichtlinie (Essential Health and Safety Requirements; EHSRs) dazu genutzt werden können, die Sicherheit von Maschinen/Anlagen anhand der Arbeitsmittel-Benutzungsrichtlinie zu bestätigen.

Dieses Kapitel behandelt Aspekte beider Richtlinien. Wer sich mit Entwurf, Lieferung, Kauf oder Einsatz industrieller Anlagen in den oder innerhalb des EWR sowie bestimmter anderer europäischer Länder befasst, sollte sich unbedingt mit den Anforderungen dieser Richtlinien vertraut machen. Die meisten Lieferanten und Betreiber von Maschinen dürfen in diese Länder nur dann Maschinen liefern bzw. in diesen Ländern Maschinen betreiben, wenn sie diese Richtlinien einhalten.

Es gelten weitere europäische Richtlinien, die für Maschinen von Bedeutung sein können. Die meisten dieser Richtlinien sind recht spezialisiert in ihrer Anwendung und werden in diesem Kapitel nicht behandelt, doch es ist wichtig zu wissen, dass auch ihre Anforderungen gegebenenfalls eingehalten werden müssen. Beispiele: Die EMV-Richtlinie 2004/108/EG und die ATEX-Richtlinie 94/9/EG.

Maschinenrichtlinie

Die Maschinenrichtlinie behandelt die Lieferung neuer Maschinen und anderer Einrichtungen einschließlich Sicherheitskomponenten. Es ist strafbar, innerhalb der EU Maschinen zu liefern, die nicht den Vorschriften und Anforderungen dieser Richtlinie entsprechen.

Die weitläufigste Definition von „Maschinen“ innerhalb dieser Richtlinie lautet wie folgt: Eine mit einem anderen Antriebssystem als der unmittelbar eingesetzten menschlichen oder tierischen Kraft ausgestattete oder dafür vorgesehene Gesamtheit miteinander verbundener Teile oder Vorrichtungen, von denen mindestens eine beweglich ist und die für eine bestimmte Anwendung zusammengefügt sind.

CE-Zeichen an Maschine angebracht

Die aktuelle Maschinenrichtline (2006/42/EG) trat Ende 2009 an die Stelle der vorherigen Version (98/37/EG). Sie wurde ergänzt und verbessert, enthält jedoch keine grundlegenden Änderungen hinsichtlich der Sicherheits- und Gesundheitsschutzanforderungen. Es gibt eine Reihe von Änderungen, die technologischen und methodischen Veränderungen Rechnung tragen. Darüber hinaus wurde die Richtlinie erweitert, um einige zusätzliche Gerätetypen abzudecken (z. B. Hebezeuge auf Baustellen). Eine Risikobeurteilung ist nun ausdrücklich erforderlich, um festzulegen, welche grundlegenden Sicherheits- und Gesundheitsschutzanforderungen anzuwenden sind, und es wurden Änderungen an den Beurteilungsverfahren für die in Anhang IV aufgeführten Maschinen implementiert.

Die wichtigsten Vorschriften der ursprünglichen Richtlinie (98/37/EG) wurden für Maschinen am 1. Januar 1995 und für Sicherheitskomponenten am 1. Januar 1997 in Kraft gesetzt.

Die Vorschriften der aktuellen Richtlinie (2006/42/EG) gelten seit dem 29. Dezember 2009. Der Hersteller oder sein bevollmächtigter Vertreter muss sicherstellen, dass die gelieferte Ausrüstung mit der Richtlinie konform ist. Dies umfasst Folgendes:

- Sicherstellen, dass die anwendbaren gesundheitlichen und sicherheitstechnischen Anforderungen in Anhang I der Richtlinie erfüllt sind
- Anlegen einer Akte mit technischer Dokumentation
- Eingehende Beurteilung der Konformität
- Ausstellen einer „EU-Konformitätserklärung“
- Anbringen des CE-Zeichens, sofern anwendbar
- Bereitstellen von Anweisungen für die sichere Verwendung

Grundlegende gesundheitliche und sicherheitstechnische Anforderungen

Maschine muss die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) erfüllen

Anhang I der Richtlinie enthält eine Liste grundlegender gesundheitlicher und sicherheitstechnischer Anforderungen (Essential Health & Safety Requirements; auch EHSRs genannt), denen die Maschinen entsprechen müssen, wo dies relevant ist. Diese Liste soll gewährleisten, dass die Maschinen sicher sind. Außerdem müssen sie so konzipiert und aufgebaut sein, dass sie in allen Phasen ihrer Nutzungsdauer betrieben, eingestellt und gewartet werden können, ohne Personen zu gefährden. Der folgende Text bietet einen kurzen Überblick über einige typische Anforderungen, doch es müssen alle in Anhang I genannten grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) erfüllt sein.

Es muss eine Risikobeurteilung durchgeführt werden, um festzustellen, welche grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen für die betreffende Ausrüstung gelten.

Die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen in Anhang I enthalten eine Hierarchie von Maßnahmen zum Ausschalten des Risikos:

(1) Eigensichere Konstruktion. Nach Möglichkeit verhindert der Aufbau selbst mögliche Gefahren.

Wo dies nicht möglich ist, sind **(2) zusätzliche Schutzgeräte**, z. B. Schutzeinrichtungen mit verriegelten Zugängen, berührungslos wirkende Barrieren wie Lichtschranken und Lichtgitter, Sensormatten usw. zu verwenden.

Jedes Restrisiko, das sich nicht mit den obigen Verfahren ausschließen lässt, muss durch **(3) persönliche Schutzausrüstung und/oder Schulung** begrenzt werden. Der Maschinenlieferant muss geeignete Maßnahmen benennen.

Für Konstruktion und Betrieb sind geeignete Materialien zu verwenden. Es sind angemessene Beleuchtung und Handhabungseinrichtungen vorzusehen. Bedienungselemente und Steuerungssysteme müssen sicher und zuverlässig sein. Maschinen dürfen nicht unerwartet anlaufen können und müssen mit einem oder mehreren Not-Halt-Geräten ausgestattet sein. Bei komplexen Anlagen ist zu berücksichtigen, wie sich vor- oder nachgeschaltete Prozesse auf die Sicherheit einer Maschine auswirken können. Der Ausfall eines Netzteils oder eines Steuerstromkreises darf nicht zu einer gefährlichen Situation führen. Maschinen müssen stabil sein und vorhersehbaren Beanspruchungen widerstehen können. Sie dürfen keine ungeschützten Kanten oder Oberflächen aufweisen, die eine Verletzungsgefahr darstellen.

Zum Schutz vor Gefahren, wie z. B. beweglichen Teilen, müssen Schutzvorrichtungen oder Schutzgeräte verwendet werden. Diese müssen von robuster Konstruktion und schwer zu

umgehen sein. Feste Schutzvorrichtungen müssen so montiert werden, dass sie nur mit Werkzeugen entfernt werden können. Bewegliche Schutzvorrichtungen müssen sicherheitsverriegelt sein. Einstellbare Schutzvorrichtungen müssen sich problemlos und ohne Werkzeuge justieren lassen.

Gefahren durch Elektrizität und andere Energiequellen müssen verhindert werden. Durch Temperatur, Explosion, Lärm, Schwingungen, Staub, Gase oder Strahlung bedingte Verletzungsgefahren sind zu minimieren. Es müssen geeignete Vorkehrungen für Wartung und Instandhaltung getroffen werden. Es sind ausreichende Anzeige- und Warngeräte vorzusehen. Maschinen sind mit Anleitungen für sichere Installation, Verwendung, Einstellung usw. zu liefern.

Beurteilung der Konformität

Der Konstrukteur, Entwickler oder eine andere akkreditierte Stelle muss nachweisen können, dass die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) erfüllt werden. Zu diesem Zweck ist eine Akte mit technischer Dokumentation anzulegen. Die technische Dokumentation muss alle relevanten Informationen wie Prüfergebnisse, Zeichnungen, Spezifikationen usw. umfassen.

Maschine muss die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) erfüllen

Eine harmonisierte europäische Norm (EN), die im Amtsblatt der Europäischen Union unter der Maschinenrichtlinie aufgelistet ist und deren Enddatum für die Annahme der Konformität noch nicht erreicht ist, geht von einer Konformität mit bestimmten EHSRs aus. (Viele neue Normen, die im Amtsblatt aufgelistet werden, umfassen einen Querverweis auf die EHSRs, die von der Norm abgedeckt werden.)

Sofern also Anlagen mit solchen aktuellen, harmonisierten europäischen Normen konform sind, ist die Aufgabe, die Konformität mit den EHSRs nachzuweisen wesentlich einfacher. Und auch der Hersteller profitiert von der besseren rechtlichen Gewissheit. Die Einhaltung dieser Normen ist nicht gesetzlich gefordert, doch ihre Anwendung ist dringend zu empfehlen, da es äußerst schwierig sein kann, die Konformität mit alternativen Verfahren nachzuweisen. Diese Normen unterstützen die Maschinenrichtlinie und werden vom CEN (Europäischen Komitee für Normung) in Zusammenarbeit mit der ISO (Internationale Organisation für Normung) und dem ENELEC (Europäisches Komitee für elektrotechnische Normung) in Zusammenarbeit mit der IEC (Internationale Kommission für Elektrotechnik) erstellt.

Eine gründliche, dokumentierte Risikobeurteilung muss durchgeführt werden, damit allen potenziellen Maschinengefahren Rechnung getragen werden kann. Auf ähnliche Weise muss der Maschinenhersteller sicherstellen, dass alle EHSRs erfüllt werden – auch jene, auf die sich keine harmonisierten EN-Normen beziehen.

Technische Dokumentation

Der Hersteller oder sein bevollmächtigter Vertreter muss eine Akte mit technischer Dokumentation anlegen, um die Konformität mit den grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) zu belegen. Die technische Dokumentation muss alle relevanten Informationen wie Prüfergebnisse, Zeichnungen, Spezifikationen usw. umfassen.

Es müssen nicht alle Informationen dauerhaft als Hardcopy vorhanden sein, doch die gesamte Akte mit technischer Dokumentation muss auf Anfrage zur Überprüfung durch eine kompetente Stelle (eine von einem EU-Land benannte Institution zur Überwachung der Konformität von Maschinen) vorgelegt werden können.

Die Akte mit der technischen Dokumentation muss mindestens folgende Dokumente umfassen:

1. Allgemeine Zeichnungen der Maschine einschließlich Pläne der Steuerstromkreise.
2. Detailzeichnungen, Berechnungsunterlagen usw., die erforderlich sind, um die Konformität der Maschine mit den grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) nachprüfen zu können.
3. Dokumentation der Risikobeurteilung, einschließlich einer Liste der für die Maschine relevanten grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) sowie eine Beschreibung der implementierten Schutzmaßnahmen.
4. Eine Liste der anwendbaren Normen und technischen Daten, die anzeigt, dass die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen abgedeckt sind.
5. Eine Beschreibung der Verfahren, mit denen die von einer Maschine ausgehenden Gefahren vermieden werden.
6. Falls gewünscht, alle technischen Berichte oder Zertifikate eines Prüfinstituts oder einer anderen Stelle.
7. Bei Erklärung der Konformität mit einer harmonisierten europäischen Norm ein technischer Bericht mit Prüfergebnissen.
8. Eine Kopie der Betriebsanleitung für die Maschine.
9. Sofern anwendbar, die Herstellererklärung für teilweise zusammengebaute Maschinen und die entsprechenden Montageanweisungen für solche Maschinen.
10. Sofern relevant, Kopien der EU-Konformitätserklärung von Maschinen oder anderen Produkten, die in die Maschine integriert wurden.
11. Eine Kopie der EU-Konformitätserklärung.

Bei Serienherstellung sind Einzelheiten zu internen Maßnahmen (z. B. Qualitätssysteme) aufzuführen, um sicherzustellen, dass alle produzierten Maschinen konform bleiben:

- Der Hersteller muss die notwendigen Untersuchungen oder Prüfungen an Komponenten, Anbauteilen oder an der fertigen Maschine durchführen, um festzustellen, ob Entwurf und Konstruktion der Maschine eine sichere Aufstellung und Inbetriebnahme erlauben.
- Die Akte mit der technischen Dokumentation muss nicht ständig in einer einzelnen Akte abgelegt sein, doch müssen die Unterlagen in angemessener Zeit zusammengestellt und vorgelegt werden können. Die Unterlagen müssen zehn Jahre nach Herstellung der letzten Einheit verfügbar sein.

Die Akte mit der technischen Dokumentation braucht keine detaillierten Pläne oder anderen speziellen Informationen zu Unterbaugruppen für die Herstellung der Maschine zu enthalten, es sei denn, dies wäre eine wesentliche Voraussetzung für die Erfüllung der grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs).

Beurteilung der Konformität von Maschinen gem. Anhang IV

Beurteilung der Konformität

Für bestimmte Arten von Maschinen/Anlagen gelten besondere Regeln. Diese Maschinen/Anlagen sind in Anhang IV der Richtlinie aufgeführt und umfassen gefährliche Maschinen wie bestimmte Holzbearbeitungsmaschinen, Pressen, Spritzgießmaschinen, unterirdisch eingesetzte Maschinen, Fahrzeughebebühnen usw.

Anhang IV umfasst auch bestimmte Sicherheitskomponenten wie Schutzeinrichtungen zum Erkennen der Präsenz von Personen (z. B. Lichtgitter) und logische Einheiten zur Gewährleistung der Sicherheitsfunktionen.

Für in Anhang IV aufgeführte Maschinen, die nicht vollständig mit den relevanten harmonisierten europäischen Normen konform sind, muss der Hersteller oder ein bevollmächtigter Vertreter eines der folgenden Verfahren anwenden:

1. EU-Baumusterprüfung. Es muss eine Akte mit technischer Dokumentation angelegt und ein Muster der Maschine bei einer akkreditierten Stelle (Prüfinstitut) zur EU-Baumusterprüfung vorgestellt werden. Besteht die Maschine die Prüfung, wird das EU-Typprüfzeugnis ausgestellt. Die Gültigkeit des Zertifikats muss alle fünf Jahre durch die akkreditierte Stelle überprüft werden.

2. Umfassende Qualitätssicherung. Es ist eine Akte mit technischer Dokumentation anzulegen und beim Hersteller muss ein genehmigtes Qualitätssystem für Konstruktion, Fertigung, Endabnahme und Prüfungen implementiert sein. Das Qualitätssystem muss die Konformität der Maschinen und die Einhaltung der Vorschriften dieser Richtlinie gewährleisten. Das Qualitätssystem muss regelmäßig durch eine akkreditierte Stelle überprüft werden.

Untersuchungen durch benannte Stelle

Für Maschinen, die nicht in Anhang IV genannt sind oder zwar in Anhang IV enthalten sind, doch vollständig mit den relevanten harmonisierten EU-Normen konform sind, hat der Hersteller oder sein bevollmächtigter Vertreter auch die Möglichkeit, die technischen Unterlagen auszuarbeiten und die Konformität der Ausrüstung selbst zu beurteilen. Es sind interne Prüfungen erforderlich, um sicherzustellen, dass die gefertigte Ausrüstung dauerhafte Konformität bietet.

Akkreditierte Stellen

In der EU wurde ein Netz akkreditierter Stellen eingerichtet, die miteinander kommunizieren und kooperieren, um gemeinsame Kriterien aufzustellen. Akkreditierte Stellen werden von Regierungen (nicht von der Industrie) ernannt. Ausführliche Informationen zu Organisationen mit dem Status einer akkreditierten Stelle finden Sie unter:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm

Verfahrensvorschrift zur EU-Konformitätserklärung

CE Das CE-Zeichen muss auf allen gelieferten Maschinen angebracht werden. Auch eine EU-Konformitätserklärung ist mit den Maschinen auszuliefern.

Das CE-Zeichen weist darauf hin, dass die Maschine mit allen anwendbaren europäischen Richtlinien konform ist und dass die Verfahren zur Beurteilung der Konformität abgeschlossen wurden. Es ist strafbar, das CE-Zeichen für die Maschinenrichtline anzubringen, wenn die Maschine die relevanten grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) nicht erfüllt.

Die EU-Konformitätserklärung muss die folgenden Informationen enthalten:

- Firmenname und vollständige Adresse des Herstellers und, sofern relevant, des bevollmächtigten Vertreters
- Name und Adresse der Person, die zum Anlegen der Akte mit technischer Dokumentation berechtigt ist und deren Geschäftssitz in der EU liegen muss (liegt der Geschäftssitz eines Herstellers außerhalb der EU, kann dies der „bevollmächtigte Vertreter“ sein)
- Beschreibung und Identifikation der Maschine, einschließlich allgemeiner Bezeichnung, Funktion, Modell, Ausführung, Seriennummer und Handelsname
- Ein Satz, der ausdrücklich erklärt, dass die Maschine alle relevanten Vorschriften dieser Richtlinie erfüllt und, sofern relevant, ein ähnlicher Satz, der die Konformität der Maschine mit anderen Richtlinien und/oder relevanten Vorschriften erklärt
- Sofern relevant, ein Verweis auf die angewandten harmonisierten Normen
- Sofern relevant, ein Verweis auf andere angewandte technische Normen und Spezifikationen
- (Für in Anhang IV aufgeführte Maschinen) sofern relevant, der Name, die Adresse und die Kennnummer der akkreditierten Stelle, die die in Anhang IX genannte EU-Baumusterprüfung ausführt, sowie die Nummer des Zertifikats der EU-Baumusterprüfung
- (Für in Anhang IV aufgeführte Maschinen) sofern relevant, der Name, die Adresse und die Kennnummer der akkreditierten Stelle, die das umfassende Qualitätssicherungssystem geprüft hat, auf das in Anhang X verwiesen wird
- Ort und Datum der Erklärung
- Die Identität und Unterschrift der Person, die die Erklärung im Namen des Herstellers oder des bevollmächtigten Vertreters ausarbeitet

EU-Herstellererklärung für teilweise zusammengebaute Maschinen

Werden Maschinenkomponenten für den Zusammenbau mit anderen Produkten geliefert, mit denen sie zu einem späteren Zeitpunkt eine komplette Maschine bilden, muss für diese eine HERSTELLERERKLÄRUNG ausgestellt werden. Das CE-Zeichen darf NICHT angebracht werden. In diesem Fall hat der Hersteller eine Erklärung mitzuliefern, in der die Inbetriebnahme der Komponenten bis zum Einbau in eine Maschine, die den Bestimmungen der Maschinenrichtlinie entspricht, untersagt wird. Es muss eine Akte mit technischer Dokumentation angelegt werden und die teilweise zusammengebaute Maschine ist mit Informationen wie der Beschreibung der Bedingungen zu versehen, die für den ordnungsgemäßen Einbau in die endgültige Maschine erfüllt sein müssen, um die Sicherheit nicht zu beeinträchtigen.

Diese Option ist nicht verfügbar für Maschinen/Anlagen, die unabhängig funktionieren können oder die Funktion einer Maschine verändern.

Die Herstellererklärung muss folgende Informationen enthalten:

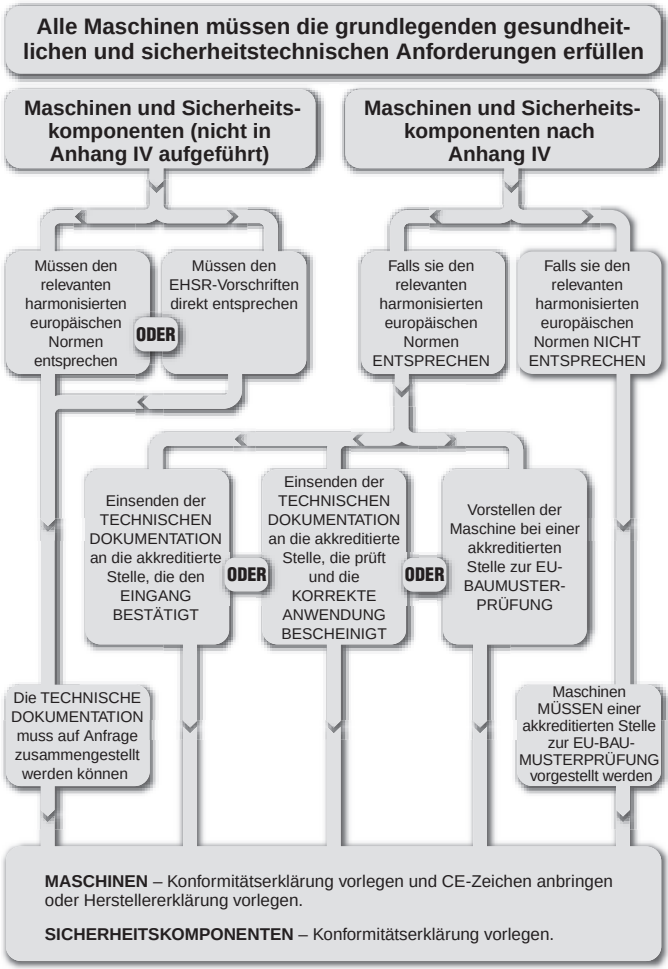
- Firmenname und vollständige Adresse des Herstellers der teilweise zusammengebauten Maschine und, sofern relevant, des bevollmächtigten Vertreters
- Name und Adresse der Person, die zum Erstellen der relevanten technischen Dokumentation berechtigt ist und deren Geschäftssitz in der EU liegen muss (liegt der Geschäftssitz eines Herstellers außerhalb der EU, kann dies der „bevollmächtigte Vertreter“ sein)
- Beschreibung und Identifikation der teilweise zusammengebauten Maschine, einschließlich allgemeiner Bezeichnung, Funktion, Modell, Ausführung, Seriennummer und Handelsname
- Ein Satz, der erklärt, welche grundlegenden Anforderungen dieser Richtlinie angewandt wurden und erfüllt sind und dass die relevante technische Dokumentation in Übereinstimmung mit Teil B von Anhang VII erstellt wurde, und, sofern relevant, ein Satz, der die Konformität der teilweise zusammengebauten Maschine mit anderen relevanten Richtlinien erklärt
- Die Zusage, die relevanten Informationen zur teilweise zusammengebauten Maschine zu übermitteln, wenn diese berechtigterweise durch staatliche Behörden angefordert werden. Diese Erklärung muss auch die Übermittlungsmethode umfassen und darf die Urheberrechte des Herstellers der teilweise zusammengebauten Maschine nicht verletzen.
- Eine Erklärung, dass die teilweise zusammengebaute Maschine erst dann in Betrieb genommen werden darf, wenn die endgültige Maschine, in die sie eingebaut werden soll, nachweislich mit den Vorschriften dieser Richtlinie konform ist, sofern relevant.
- Ort und Datum der Erklärung
- Die Identität und Unterschrift der Person, die die Erklärung im Namen des Herstellers oder des bevollmächtigten Vertreters ausarbeitet.

Maschinen, die von außerhalb der EU geliefert werden – bevollmächtigte Vertreter

Wenn ein Hersteller, dessen Geschäftssitz außerhalb der EU (oder des EWR) liegt, Maschinen in die EU exportiert, muss er einen bevollmächtigten Vertreter benennen.

Ein bevollmächtigter Vertreter ist eine natürliche oder juristische Person mit Geschäftssitz in der EU, die über eine schriftliche Vollmacht des Herstellers verfügt, in seinem Namen alle oder einen Teil der Verpflichtungen und Formalitäten im Rahmen der Maschinenrichtlinie abzuwickeln.

Die Arbeitsmittel-Benutzungsrichtlinie der EU


Alle Maschinen müssen die grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen erfüllen
Maschinen und Sicherheitskomponenten (nicht in Anhang IV aufgeführt)
Maschinen und Sicherheitskomponenten nach Anhang IV
Müssen den relevanten harmonisierten europäischen Normen entsprechen
ODER
Müssen den EHSR-Vorschriften direkt entsprechen
Falls sie den relevanten harmonisierten europäischen Normen ENTSPRECHEN
Falls sie den relevanten harmonisierten europäischen Normen NICHT ENTSPRECHEN
Einsenden der TECHNISCHEN DOKUMENTATION an die akkreditierte Stelle, die den EINGANG BESTÄTIGT
ODER
Einsenden der TECHNISCHEN DOKUMENTATION an die akkreditierte Stelle, die prüft und die KORREKTE ANWENDUNG BESCHEINIGT
ODER
Vorstellen der Maschine bei einer akkreditierten Stelle zur EU-BAUMUSTER-PRÜFUNG
Die TECHNISCHE DOKUMENTATION muss auf Anfrage zusammengestellt werden können
Maschinen MÜSSEN einer akkreditierten Stelle zur EU-BAU-MUSTERPRÜFUNG vorgestellt werden
MASCHINEN – Konformitätserklärung vorlegen und CE-Zeichen anbringen oder Herstellererklärung vorlegen.
SICHERHEITSKOMPONENTEN – Konformitätserklärung vorlegen.

Übersicht zum Verfahren der Maschinenrichtlinie

Während die Maschinenrichtlinie für die Lieferanten gedacht ist, zielt diese Richtlinie (89/655/EWG, geändert durch 95/63/EG, 2001/45/EG und 2007/30/EG) auf die Anwender der Maschinen ab. Sie deckt sämtliche Industriesektoren ab und formuliert allgemeine Verpflichtungen für Arbeitgeber, was auch die Einhaltung von Mindestanforderungen für die Sicherheit von Arbeitsmitteln umfasst. Alle EU-Länder erlassen eigene Gesetze, um diese Richtlinie umzusetzen.

Es wird beispielsweise auf ihre Realisierung in Großbritannien unter dem Namen „The Provision and Use of Work Equipment Regulations“ (PUWER) eingegangen. Die Form der Realisierung kann von Land zu Land unterschiedlich sein, doch die Wirkung der Richtlinie bleibt unverändert.

Die Artikel der Richtlinie erläutern im Einzelnen, für welche Arten von Maschinen/Anlagen und Arbeitsplätzen die Richtlinie gilt.

Sie definieren auch allgemeine Pflichten der Arbeitgeber, wie den Einsatz sicherer Arbeitssysteme und die Bereitstellung geeigneter und sicherer Arbeitsmittel, die ordnungsgemäß instand gehalten werden müssen. Maschinenbedienern müssen geeignete Informationen und Schulungen für das sichere Arbeiten mit der Maschine zur Verfügung gestellt werden.

Neue Maschinen (und Gebrauchtmaschinen von außerhalb der EU), die nach dem 1. Januar 1993 geliefert wurden, müssen die relevanten Produktrichtlinien erfüllen, z. B. die Maschinenrichtlinie (laut Übergangsbestimmungen). Aus einem Land der EU stammende Gebrauchtmaschinen, die erstmals in Verkehr gebracht werden, müssen sofort die Mindestanforderungen erfüllen, die im Anhang der Arbeitsmittel-Benutzungsrichtlinie aufgeführt sind.

Hinweis: Ältere oder gebrauchte Maschinen, die wesentlich verändert, überholt oder umgebaut werden, gelten als neue Maschinen und müssen damit der Maschinenrichtlinie entsprechen (auch wenn sie nur innerhalb des Unternehmens eingesetzt werden).

Die Eignung der Arbeitsmittel ist eine wichtige Anforderung der Richtlinie und betont die Verantwortung des Arbeitgebers, eine sachgerechte Risikobeurteilung durchzuführen.

Eine Maschine muss ordnungsgemäß gewartet werden. Dies bedeutet normalerweise, dass ein Programm für die routine- und planmäßige Instandhaltung existieren muss. Es wird empfohlen, Maschinenbücher zu führen und auf dem neuesten Stand zu halten. Dies ist besonders dann wichtig, wenn die Wartung und Prüfung von Maschinen/Anlagen zur kontinuierlichen Sicherheitsintegrität von Schutzeinrichtungen oder Schutzsystemen beiträgt.

Der Anhang der Arbeitsmittel-Benutzungsrichtlinie stellt allgemeine Mindestanforderungen an Arbeitsmittel.

Wenn die Arbeitsmittel mit relevanten Produktrichtlinien konform sind, z. B. mit der Maschinenrichtlinie, erfüllen sie automatisch die entsprechenden Mindestanforderungen an den Maschinenaufbau, die im Anhang genannt sind.

Mitgliedsstaaten dürfen Gesetze zur Nutzung von Arbeitsmitteln erlassen, die über die Mindestanforderungen der Arbeitsmittel-Benutzungsrichtlinie hinausgehen.

Ausführliche Informationen zur Verwendung der Arbeitsmittel-Benutzungsrichtlinie finden Sie auf der offiziellen EU-Webseite:

http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

US-Vorschriften

Dieser Abschnitt stellt einige US-amerikanische Vorschriften für Sicherheitseinrichtungen an industriellen Maschinen vor. Dies ist nur einer von vielen möglichen Ansatzpunkten. Die Anforderungen für die jeweiligen Anwendungen müssen im Einzelfall eingehender untersucht werden. Durch geeignete Maßnahmen ist sicherzustellen, dass die Verfahren für Entwurf, Betrieb und Instandhaltung sowohl den eigenen Bedürfnissen als auch den nationalen und lokalen Vorschriften und Normen entsprechen.

In den USA gibt es eine Vielzahl von Organisationen zur Förderung der technischen Sicherheit. Hierzu gehören:

1. Unternehmen, die sich nach bestehenden Anforderungen richten und auch eigene interne Anforderungen formulieren;

2. Occupational Safety and Health Administration (OSHA): US-amerikanische Organisation für sichere und gesunde Bedingungen am Arbeitsplatz;

3. Industrieorganisationen, z. B. National Fire Protection Association (NFPA) für Brandschutz, Robotics Industries Association (RIA) für Robotertechnik und die Association of Manufacturing Technology (AMT) für Fertigungstechnik; dazu Lieferanten sicherheitstechnischer Produkte und Lösungen wie Rockwell Automation.

Occupational Safety and Health Administration (OSHA)

In den Vereinigten Staaten ist die Occupational Safety and Health Administration (OSHA) eine der wichtigsten Institutionen zur Durchsetzung sicherheitstechnischer Anforderungen. Die OSHA wurde 1970 per Gesetz vom US-Kongress ins Leben gerufen. Zweck dieses Gesetzes ist es, sichere und gesunde Arbeitsbedingungen zu schaffen und Menschen an ihrem Arbeitsplatz zu schützen. Dieses Gesetz bevollmächtigt den Arbeitsminister, verbindliche gesundheitliche und sicherheitsbezogene Arbeitsnormen festzulegen, die für Unternehmen gelten, die zwischenstaatlichen Handel betreiben. Dieses Gesetz findet Anwendung hinsichtlich der Beschäftigung an einem Arbeitsplatz in einem US-Bundesstaat, im Bundesdistrikt Columbia, im Commonwealth von Puerto Rico, auf den Amerikanischen Jungferninseln, in Amerikanisch-Samoa, Guam, in Amerikanisch-Ozeanien, auf Wake Island und in den Ländern des Outer Continental Shelfs wie im Outer Continental Shelf Lands Act definiert, auf Johnston Island und in der Kanalzone.

Artikel 5 des Gesetzes legt die grundlegenden Anforderungen fest. Er besagt, dass jeder Arbeitgeber jedem seiner Mitarbeiter Arbeit und einen Arbeitsplatz bereitstellen muss, die frei

von bekannten Gefahren sind, welche zum Tod oder zu ernsten gesundheitlichen Schäden des Mitarbeiters führen oder führen können. Außerdem muss er sich an die in diesem Gesetz dargelegten Normen zur Sicherheit und Gesundheit am Arbeitsplatz halten.

Artikel 5 besagt außerdem, dass jeder Mitarbeiter die Normen zur Sicherheit und Gesundheit am Arbeitsplatz sowie alle Richtlinien, Vorschriften und im Sinne dieses Gesetzes ausgesprochene Anweisungen einhalten muss, die sich auf seine eigenen Handlungen und sein Verhalten beziehen.

Das OSHA-Gesetz verpflichtet also den Arbeitgeber ebenso wie den Arbeitnehmer. Darin unterscheidet sich dieses Gesetz von der Maschinenrichtlinie, gemäß der Lieferanten nur Maschinen auf den Markt bringen dürfen, die frei von Gefahren sind. In den USA kann ein Lieferant eine Maschine auch ohne jede Schutzeinrichtung verkaufen. Der Nutzer ist verpflichtet, die Schutzeinrichtung zu ergänzen, damit die Maschine sicher ist. Auch wenn dies gängige Praxis war, als das Gesetz verabschiedet wurde, geht der Trend bei den Lieferanten dahin, Maschinen mit den Schutzeinrichtungen zur Verfügung zu stellen, da die Planung einer Maschine mit Sicherheitsvorkehrungen wesentlich kostengünstiger ist als die Ergänzung der Schutzeinrichtungen nach der Entwicklung und dem Bau der Maschine. Normen versuchen jetzt, Lieferanten und Nutzer dazu zu bringen, über Anforderungen für Schutzeinrichtungen zu sprechen, damit die Maschinen nicht nur sicher, sondern auch produktiver werden.

Der Arbeitsminister ist befugt, alle nationalen Konsensnormen sowie alle geltenden bundesweiten Normen als Normen für sichere und gesunde Bedingungen am Arbeitsplatz zu veröffentlichen, es sei denn, die Veröffentlichung einer solchen Norm führt nicht zu verbesserten Sicherheits- und Gesundheitsbedingungen für bestimmte Mitarbeiter.

Die OSHA bewältigt diese Aufgabe durch Herausgeben von Vorschriften im Bundesgesetzblatt der USA (Titel 29 CFR). Normen für industrielle Maschinen werden durch die OSHA in Teil 1910 von 29 CFR veröffentlicht. Diese stehen kostenlos über die OSHA-Webseite unter www.osha.gov zur Verfügung. Im Gegensatz zu den meisten Normen, deren Einhaltung freiwillig ist, gelten die Normen der OSHA als Gesetze.

Im Folgenden sind einige wichtige Teile aufgeführt, die für die Maschinensicherheit gelten:

- A – Allgemeines
- B – Anpassung und Erweiterung der geltenden bundesweiten Normen
- C – Allgemeine Sicherheits- und Gesundheitsverordnungen
- H – Gefährliche Materialien
- I – Persönliche Schutzausrüstung
- J – Allgemeine Umgebungsüberwachung – einschließlich Verriegelung/Kennzeichnung (Lockout/Tagout)
- O – Anlagen- und Maschinenschutz
- R – Spezielle Industrien
- S – Elektrik

Einige OSHA-Normen verweisen auf freiwillige Normen. Die Berücksichtigung durch Verweise hat gesetzlich die Auswirkung, dass das Material gehandhabt wird, als ob es vollständig im Bundesregister eingetragen wäre. Wenn eine nationale Konsensnorm per Verweis in einem der Teilsätze erwähnt wird, gilt diese Norm als Gesetz. Beispielsweise wird im Teilsatz S auf NFPA 70 verwiesen – eine freiwillige Norm, die als US National Electric Code (NEC) bekannt ist. Daher sind die Anforderungen in der Norm NFPA 70 verbindlich.

29 CFR 1910.147 in Teilsatz J deckt die Kontrolle gefährlicher Energie ab. Dieser ist im Allgemeinen auch als Norm für Verriegelung/Kennzeichnung nach Trennung von der Energiequelle (Lockout/Tagout) bekannt. Die äquivalente freiwillige Norm hierzu lautet ANSI Z244.1. Grundsätzlich fordert diese Norm, dass die Energieversorgung einer Maschine abgeschaltet wird, wenn Wartungs- oder Instandhaltungsarbeiten ausgeführt werden. Zweck dieser Norm ist es, ein unerwartetes Einschalten und Anlaufen der Maschine zu verhindern, was zur Verletzung der Mitarbeiter führen würde.

Die Mitarbeiter müssen ein Programm ausarbeiten und mithilfe bestimmter Verfahren geeignete Verriegelungen oder Abschaltgeräte anbringen, um die Geräte von der Energieversorgung zu isolieren und um andererseits zu verhindern, dass die Maschinen oder Anlagen sich unerwartet einschalten, unerwartet anlaufen oder gespeicherte Energie freisetzen und Mitarbeiter verletzen.

Geringe Änderungen und Anpassungen der Werkzeuge sowie weitere kleine Wartungsarbeiten, die während des normalen Produktionsbetriebs stattfinden, werden nicht durch diese Norm abgedeckt, sofern es sich um routinemäßige, regelmäßige Arbeiten handelt, die Teil der normalen Verwendung der Anlagen in der Produktion sind. Voraussetzung hierfür ist, dass die Arbeiten mithilfe alternativer Maßnahmen ausgeführt werden, die einen effizienten Schutz bieten. Alternative Maßnahmen sind beispielsweise Schutzeinrichtungen wie Lichtgitter, Schaltmatten, Schutztür-Verriegelungsüberwachungen und ähnliche Geräte, die an ein Sicherheitssystem angeschlossen sind. Der Maschinenentwickler und -anwender muss dabei bestimmen, was „kleinere“ Arbeiten sind und was unter „routinemäßig, regelmäßig und Teil der normalen Verwendung“ zu verstehen ist.

Teilsatz O deckt „Anlagen- und Maschinenschutz“ ab. In diesem Teilsatz sind die allgemeinen Anforderungen für alle Maschinen sowie die Anforderungen für einige spezielle Maschinen aufgeführt. Als die OSHA im Jahr 1970 gegründet wurde, übernahm sie zahlreiche bestehende ANSI-Normen. Beispielsweise wurde B11.1 für weggebundene Pressmaschinen als 1910.217 übernommen.

1910.212 ist die allgemeine OSHA-Norm für Maschinen. Sie besagt, dass eine oder mehrere Methoden für den Maschinenschutz vorgesehen werden müssen, um den Bediener und andere Mitarbeiter im Maschinenbereich vor Gefahren zu schützen, die beispielsweise vom Arbeitsraum, von nach innen gerichteten Quetschpunkten, drehenden Teilen sowie Span- und Funkenflug ausgehen. Die Schutzvorrichtungen müssen, sofern möglich, an der Maschine angebracht werden. Ist dies aus irgendwelchen Gründen nicht möglich, sind die Schutzvorrichtungen an anderer Stelle anzubringen. Die Schutzvorrichtung muss so ausgelegt sein, dass durch sie selbst keine Unfallgefahr ausgeht.

Der „Arbeitsraum“ ist der Bereich einer Maschine, in dem das Material tatsächlich bearbeitet wird. Der Arbeitsraum einer Maschine, dessen Betrieb die Verletzung eines Mitarbeiters zur Folge haben kann, muss mit einer Sicherheitsvorrichtung geschützt werden. Die Sicherheitsvorrichtung muss mit eventuell geltenden Normen übereinstimmen oder, sofern keine bestimmten Normen vorliegen, so konzipiert und konstruiert sein, dass sie das Eindringen von Körperteilen eines Mitarbeiters in die Gefahrenzone während des Betriebszyklus verhindert.

In Teilsatz S (1910.399) sind die elektrischen Anforderungen der OSHA angeführt. Eine Installation oder Anlage wird vom stellvertretenden Arbeitsminister anerkannt und im Sinne dieses Teilsatzes S genehmigt, wenn sie durch ein national anerkanntes Testlabor akzeptiert, zertifiziert, aufgelistet, gekennzeichnet oder anderweitig als sicher bestimmt wird.

Was sind Anlagen? Ein allgemeiner Begriff, der sich auf Material, Befestigungselemente, Geräte, Einrichtungen, Halterungen, Vorrichtungen, Apparate und ähnliche Elemente bezieht, die als Teil oder in Verbindung mit einer elektrischen Installation verwendet werden.

Was bedeutet „aufgelistet“? Anlagen gelten als „aufgelistet“, wenn sie in irgendeiner Weise in einer Liste erwähnt werden, die (a) durch ein national anerkanntes Labor veröffentlicht wird, das regelmäßig die Produktion solcher Anlagen überprüft und (b) aussagen, dass diese Anlagen national anerkannte Normen erfüllen oder getestet wurden und ihre Verwendung auf eine bestimmte Weise als sicher gilt.

Seit August 2009 gelten die folgenden Unternehmen als durch die OSHA national anerkannte Testlabors:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TÜV America, Inc. (TÜVAM)
- TÜV Product Services GmbH (TÜVPSG)
- TÜV Rheinland of North America, Inc. (TÜV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Einige Staaten haben ihre eigenen lokalen OSHAs übernommen. 24 Staaten, Puerto Rico und die Amerikanischen Jungferninseln verfügen über von der OSHA genehmigte Staatspläne und haben ihre eigenen Normen und Durchsetzungsmethoden. Zum großen Teil übernehmen diese Staaten Normen, die mit denen der bundesweiten OSHA identisch sind. Allerdings haben

einige Staaten hinsichtlich dieses Themas andere Normen übernommen oder verfügen über andere Durchsetzungsmethoden. Die Arbeitgeber müssen eventuelle Vorfälle der OSHA melden. Die OSHA stellt die Häufigkeit solcher Vorfälle zusammen und leitet diese Informationen an die lokalen Behörden weiter. Außerdem nutzt sie diese Informationen, um Prioritäten für Untersuchungen festzulegen. Die wichtigsten Faktoren für Untersuchungen sind:

- Unmittelbare Gefahr
- Katastrophen und Todesfälle
- Beschwerden von Mitarbeitern
- Industrien mit hohem Gefahrenpotenzial
- Lokale geplante Untersuchungen
- Nachuntersuchungen
- Programme mit nationalem und lokalem Schwerpunkt

Verletzungen der OSHA-Normen können mit Geldstrafen geahndet werden. Dabei gelten folgende Abstufungen:

- Ernsthaft: bis 7000 US-$ pro Verletzung der Norm
- Andere (nicht ernsthaft): nach Ermessen, jedoch maximal 7000 US-$
- Wiederholte Verletzungen: bis zu 70 000 US-$ pro Verletzung der Norm
- Vorsätzlich: bis zu 70 000 US-$ pro Verletzung der Norm
- Verletzungen der Norm, die zu Todesfällen führen: weitere Strafen
- Nichtbeseitigung der Ursachen: 7000 US-$ pro Tag

In der folgenden Tabelle sind die 14 am häufigsten zitierten OSHA-Normen zwischen Oktober 2004 und September 2005 aufgeführt.

Norm	Beschreibung
1910.147	Kontrolle gefährlicher Energie (Verriegelung/Kennzeichnung)
1910.1200	Mitteilung von Gefahren
1910.212	Allgemeine Anforderungen für alle Maschinen
1910.134	Atemschutz
1910.305	Verdrahtungsmethoden, Komponenten und Anlagen für die allgemeine Verwendung
1910.178	Industrielle Flurförderer mit Kraftantrieb
1910.219	Mechanische Antriebselemente
1910.303	Allgemeine Anforderungen
1910.213	Holzbearbeitungsmaschinen
19102.215	Schleifscheibenmaschinen
19102.132	Allgemeine Anforderungen
1910.217	Weggebundene Pressmaschinen
1910.095	Geräuschpegel am Arbeitsplatz
1910.023	Schutzöffnungen und -hohlräume in Böden und Wänden

Kanadische Vorschriften

In Kanada wird die industrielle Sicherheit auf Provinzebene geregelt. Jede Provinz verfügt über ihre eigenen Vorschriften, die verwaltet und durchgesetzt werden. Beispielsweise hat Ontario den Occupational Health and Safety Act (Gesetz für Sicherheit und Gesundheit am Arbeitsplatz) verabschiedet, der die Rechte und Pflichten aller Parteien am Arbeitsplatz definiert. Sein Hauptzweck ist der Schutz der Arbeiter vor Gesundheits- und Sicherheitsrisiken am Arbeitsplatz. Das Gesetz sieht Maßnahmen für den Umgang mit Gefahren am Arbeitsplatz vor und bietet Maßnahmen zur Durchsetzung des Gesetzes, wenn es nicht freiwillig eingehalten wird.

Teil des Gesetzes ist Vorschrift 851, Abschnitt 7, in dem die Überprüfung der Gesundheits- und Sicherheitsrisiken vor der Inbetriebnahme definiert ist. Diese Überprüfung ist in Ontario Pflicht für alle neuen, überarbeiteten oder geänderten Maschinenteile. Es muss ein Bericht von einem qualifizierten Ingenieur erstellt werden.

Normen

Dieser Abschnitt enthält eine Liste einiger typischer internationaler und nationaler Normen, die für die Maschinensicherheit relevant sind. Diese Liste erhebt keinen Anspruch auf Vollständigkeit, sondern soll lediglich einen Eindruck vermitteln, welche Maschinensicherheitsfragen Thema der Standardisierung sind.

Dieser Abschnitt sollte in Verbindung mit dem Abschnitt „Vorschriften“ gelesen werden.

Die Länder dieser Welt streben eine globale Harmonisierung der Normen an. Dies wird vor allem im Bereich der Maschinensicherheit deutlich. Weltweite Sicherheitsnormen für Maschinen werden von zwei Organisationen bestimmt: ISO und IEC. Regionale und landesweite Normen bestehen weiterhin und unterstützen auch in Zukunft lokale Anforderungen. Doch in zahlreichen Ländern geht der Trend hin zur Verwendung internationaler Normen, die von der ISO und der IEC formuliert wurden.

Beispielsweise werden die EN-Normen (europäische Norm) in den Ländern des EWR angewandt. Alle neuen EN-Normen orientieren sich an den ISO- und IEC-Normen und weisen in den meisten Fällen auch identische Formulierungen auf.

IEC-Normen decken elektrotechnische Fragen ab, während ISO-Normen alle anderen Bereiche abdecken. Die meisten industrialisierten Länder sind Mitglieder der IEC und der ISO. Normen zur Maschinensicherheit werden von Arbeitsgruppen geschrieben, die aus Experten aus vielen Industrienationen der Welt bestehen.

In den meisten Ländern gilt die Einhaltung von Normen als freiwillig, während Vorschriften rechtlich verbindlich sind. Allerdings werden Normen in der Regel als praktische Interpretation der Vorschriften verwendet. Daher sind die Welten der Normen und Vorschriften eng miteinander verbunden.

Eine umfassende Liste mit Normen finden Sie im Sicherheitskatalog, der unter www.ab.com/safety zur Verfügung steht.

ISO (International Organization for Standardization)

Die ISO ist eine nichtstaatliche Organisation, die aus den nationalen Normungseinrichtungen der meisten Länder der Welt besteht (157 Länder zum Zeitpunkt der Drucklegung dieses Dokuments). Ein zentrales Sekretariat mit Sitz in Genf koordiniert das System. Die ISO arbeitet Normen für die effizientere, sicherere und sauberere Entwicklung, Produktion und Nutzung von Maschinen aus. Darüber hinaus machen die Normen den Handel zwischen den Ländern einfacher und gerechter. ISO-Normen können durch die drei Buchstaben ISO identifiziert werden.

Die ISO-Maschinennormen sind genau wie die EN-Normen auch in drei Ebenen unterteilt: Typ A, B und C (siehe den späteren Abschnitt zu harmonisierten europäischen EN-Normen).

Weitere Informationen finden Sie auf der ISO-Webseite: *www.iso.org*.

IEC (International Electrotechnical Commission)

Die IEC ist für die Ausarbeitung und Veröffentlichung internationaler Normen für elektrische, elektronische und zugehörige Technologien zuständig. Durch ihre Mitglieder fördert die IEC die internationale Zusammenarbeit bei allen Fragen der elektrotechnischen Standardisierung und damit zusammenhängenden Angelegenheiten, wie z. B. die Beurteilung der Konformität mit elektrotechnischen Normen.

Weitere Informationen finden Sie auf der IEC-Webseite: www.iec/ch

Harmonisierte europäische EN-Normen

Diese Normen gelten für alle Länder des EWR und werden von den europäischen Normungs-instituten CEN und CENELEC ausgearbeitet. Ihre Anwendung ist freiwillig, doch die Konstruktion und Herstellung von Maschinen/Anlagen unter Beachtung dieser Normen ist der direkteste Weg, die Erfüllung der grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) der Maschinenrichtlinie nachzuweisen.

Sie sind in drei 3 Typen unterteilt: A, B und C.

NORMEN vom Typ A: behandeln Gesichtspunkte, die alle Arten von Maschinen betreffen.

NORMEN vom Typ B: Nochmals in zwei Gruppen unterteilt.
Normen vom Typ B1: behandeln insbesondere sicherheitsbezogene und ergonomische Gesichtspunkte von Maschinen.
Normen vom Typ B2: behandeln Sicherheitskomponenten und Schutzeinrichtungen.

NORMEN vom Typ C behandeln bestimmte Arten oder Gruppen von Maschinen.

Es ist wichtig zu wissen, dass bei Erfüllung einer Norm der Gruppe C automatisch von der Konformität mit den grundlegenden gesundheitlichen und sicherheitstechnischen Anforderungen (EHSRs) ausgegangen wird. In Abwesenheit einer geeigneten Norm der Gruppe C können Normen der Gruppen A und B herangezogen werden, um teilweise oder vollständig den Nachweis der EHSR-Konformität zu erbringen, indem auf Konformität mit relevanten Abschnitten verwiesen wird.

Es wurden Vereinbarungen für die Kooperation zwischen CEN/CENELEC und Organisationen wie der ISO und der IEC getroffen. Dies sollte letztendlich zu gemeinsamen, weltweit gültigen Normen führen. In den meisten Fällen gibt es für eine EN-Norm eine IEC- oder ISO-Entsprechung. Im Allgemeinen sind die beiden Texte identisch. Auf eventuelle regionale Unterschiede wird im Vorwort der Norm hingewiesen.

Eine umfassende Liste der EN-Normen zur Maschinensicherheit finden Sie unter:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm.

US-Normen

OSHA-Normen

Wo möglich, verkündigt die OSHA nationale Konsensnormen oder bestehende Bundesnormen als Sicherheitsnormen. Die verbindlichen Bestimmungen (z. B. weist das Wort „shall“ auf Verbindlichkeit hin) der Normen, die durch Verweise integriert wurden, haben dieselbe Kraft und Auswirkung wie die in Teil 1910 aufgeführten Normen. Beispielsweise wird die nationale Konsensnorm NFPA 70 als Referenzdokument in Anhang A von Teilsatz S (Teil von 1910 von 29 CFR zur Elektrik) genannt. NFPA 70 ist eine freiwillige Norm, die von der NFPA (National Fire Protection Association) entwickelt wurde. NFPA 70 ist auch als National Electric Code (NEC) bekannt und enthält Vorschriften für die Elektrotechnik. Durch die Integration werden alle verbindlichen Anforderungen im NEC auch für die OSHA-Normen verbindlich.

ANSI-Normen

Das Amerikanische Institut für Normung (American National Standards Institute, Abk. ANSI) verwaltet und koordiniert das Normungswesen für den privaten Sektor in den USA. Es handelt sich um eine gemeinnützige Vereinigung, die durch diverse private und öffentliche Organisationen unterstützt wird.

Das ANSI selbst entwickelt keine Normen, sondern erleichtert deren Entwicklung durch die Schaffung eines Konsenses zwischen qualifizierten Gruppen. ANSI gewährleistet auch, dass Leitsätze wie Konsensfähigkeit, Zweckmäßigkeit und Offenheit von den betroffenen Gruppen befolgt werden. Es folgt eine (nicht vollständige) Liste industrieller Sicherheitsnormen, die über ANSI bezogen werden können.

Diese Normen werden entweder als Anwendungsnormen oder als Ausführungsnormen kategorisiert. Die Anwendungsnormen definieren, wie eine Schutzeinrichtung an Maschinen angebracht wird. Beispiele sind ANSI B11.1 (Informationen zum Einsatz von Sicherheitseinrichtungen an Pressmaschinen) und ANSI/RIA R15.06 (Schutzeinrichtungen für Roboter).

National Fire Protection Association (Brandschutz)

Die National Fire Protection Association (NFPA) wurde 1896 gegründet. Dieser Verband widmet sich der Aufgabe, die Beeinträchtigung der Lebensqualität durch Brände zu reduzieren, und tritt zu diesem Zweck für wissenschaftlich fundierte Konsensgesetze und -normen, Forschung und Ausbildung im Bereich des Brandschutzes und damit zusammenhängende Sicherheitsmaßnahmen ein. Die NFPA fördert die Ausarbeitung vieler Normen, um diese Aufgabe zu erfüllen. Zwei sehr wichtige Normen für technische Sicherheit und Sicherheitseinrichtungen sind National Electric Code (Nationale elektrotechnische Vorschrift) und Electrical Standard for Industrial Machinery (Elektrotechnische Norm für industrielle Maschinen).

Die National Fire Protection Association unterstützt den NEC seit 1911. Das ursprüngliche Gesetzesdokument war 1897 das Ergebnis der vereinten Anstrengungen verschiedener Interessenvertreter aus Versicherungswesen, Elektrotechnik und Bauwesen. Der NEC wurde seitdem mehrmals aktualisiert. Er wird etwa alle drei Jahre überarbeitet. NEC-Artikel 670 enthält einige Details zu industriellen Maschinen und verweist auf die Norm „Electrical Standard for Industrial Machinery, NFPA 79“.

NFPA 79 gilt für elektrische/elektronische Geräte, Apparate oder Systeme von industriellen Maschinen, die mit einer Nennspannung von 600 Volt oder weniger arbeiten. Zweck von NFPA 79 ist das Bereitstellen ausführlicher Informationen für die Verwendung elektrischer/elektronischer Geräte, Apparate oder Systeme, die als Teil industrieller Maschinen geliefert werden. Diese Informationen sollen dazu beitragen, Leben und Sachwerte zu schützen. Die Norm NFPA 79 wurde 1962 offiziell vom ANSI übernommen und ähnelt inhaltlich sehr der Norm IEC 60204-1.

Von Maschinen, die keinen bestimmten OSHA-Normen unterliegen, wird gefordert, dass sie frei von erkannten Gefahren sind, die tödliche oder schwere Verletzungen verursachen können. Diese Maschinen müssen so ausgelegt und gewartet werden, dass sie die Anforderungen der anwendbaren Industrienormen erfüllen. NFPA 79 ist eine Norm für Maschinen, auf die keine OSHA-Norm anwendbar ist.

Kanadische Normen

CSA-Normen (Canadian Standard Association) spiegeln einen nationalen Konsens von Herstellern und Anwendern wider – hierzu zählen unter anderem auch Fertigungsunternehmen, Verbraucher, Einzelhändler, Gewerkschaften und professionelle Organisationen sowie Regierungsbehörden. Die Normen sind in Industrie und Handel weit verbreitet und wurden oft von kommunalen, provinziellen und bundesweiten Behörden in deren Vorschriften übernommen. Dies gilt insbesondere für die Bereiche Gesundheit, Sicherheit, Bau und Umwelt.

Einzelpersonen, Unternehmen und Vereinigungen in ganz Kanada haben der Normenentwicklung der CSA ihre Unterstützung zugesichert, indem sie der Arbeit des CSA-Komitees ihre Zeit und Qualifikation freiwillig zur Verfügung stellen und die Ziele der Vereinigung durch langfristige Mitgliedschaften unterstützen. Die über 7000 Freiwilligen des Komitees sowie die 2000 langfristigen Mitgliedschaften bilden zusammen die Gesamtmitgliederzahl der CSA.

Der Standards Council of Canada ist das koordinierende Gremium des National-Standards-Systems. Hierbei handelt es sich um eine Vereinigung unabhängiger, autonomer Organisationen, die sich für die weitere Entwicklung und Verbesserung der freiwilligen Standardisierung im nationalen Interesse einsetzen.

Australische Normen

Die meisten dieser Normen orientieren sich stark an den entsprechenden ISO-/IEC-/EN-Normen

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001, Australien
Telefon: +61 2 8206 6000
E-Mail: mail@standards.org.au
Webseite: www.standards.org.au

Kopien der Normen können Sie über folgende Adresse beziehen:
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001, Australien
Telefon: +61 2 8206 6000
Fax: +61 2 8206 6001
E-Mail: mail@sai-global.com
Webseite: www.saiglobal.com/shop

Eine umfassende Liste mit Normen finden Sie im Sicherheitskatalog, der unter www.ab.com/safety zur Verfügung steht.

Sicherheitsstrategie

Wenn man ausschließlich die Funktion einer Maschine betrachtet, ist sie umso besser, je effizienter sie Material verarbeitet. In der Praxis muss eine Maschine aber auch sicher sein. Die Sicherheit ist ein primärer Gesichtspunkt.

Zur Ausarbeitung einer ordnungsgemäßen Sicherheitsstrategie sind zwei Hauptschritte erforderlich, die wie unten dargestellt zusammenarbeiten.

RISIKOBEURTEILUNG
Alle Maschinen im Arbeitsbereich identifizieren – dann für jede Maschine
Relevante Informationen und Gutachten einholen
GRENZEN DER MASCHINE
Sind alle möglichen Betriebszustände und Einsatzsituationen der Maschine vorhersehbar?
NEIN
JA
GEFAHREN ERKENNEN
Jede denkbare Gefahrensituation erkennen – Anschließend für jede Gefahr
RISIKOABSCHÄTZUNG
Höhe des durch die Gefahr bedingten Risikos abschätzen
RISIKOMINDERUNG
RISIKO BEWERTEN
Ist die Höhe des Risikos akzeptabel?
NEIN
Der Gefahr durch Entwurfsänderung oder zusätzliche Maßnahmen begegnen
Wurden Sicherheitsmaßnahmen analysiert und als angemessen beurteilt?
NEIN
Feststellen, ob Wirkung und funktionale Eigenschaften der Sicherheitsmaßnahmen geeignet für die Maschine und ihr Einsatzprofil sind
JA
ENDE DES PROZESSES
SICHERHEITSSTRATEGIE

RISIKOBEURTEILUNG auf der Grundlage eines klaren Verständnisses der Maschinenfunktionen und der Festlegung der Maschinengrenzwerte sowie der Kenntnisse der Arbeiten.

Anschließend erfolgt die **RISIKOMINDERUNG**, sofern erforderlich. Dabei richtet sich die Auswahl von Sicherheitsmaßnahmen nach den in der Phase der Risikobeurteilung gewonnenen Informationen. Die Art und Weise, in der dies geschieht, ist die Grundlage der SICHERHEITSSTRATEGIE für die Maschine.

Dazu wird eine Checkliste benötigt, um sicherzustellen, dass alle Gesichtspunkte berücksichtigt werden und sich das übergeordnete Prinzip nicht im Detail verliert. Der gesamte Prozess muss dokumentiert werden. Dies gewährleistet nicht nur eine gründlichere Erledigung der Aufgabe, sondern macht auch die Ergebnisse für die Überprüfung durch andere Beteiligte verfügbar.

Dieser Abschnitt bezieht sich auf Maschinenhersteller und auf Maschinenanwender. Der Hersteller muss sicherstellen, dass seine Maschine sicher verwendet werden kann. Die Risikobeurteilung muss bereits während der Entwicklungsphase der Maschine beginnen und alle vorhersehbaren Aufgaben berücksichtigen, die an der Maschine ausgeführt werden müssen. Dieses aufgabenbasierte Konzept in der frühen Phase der Risikobeurteilung ist äußerst wichtig. Beispielsweise müssen eventuell bewegliche Teile an der Maschine regelmäßig justiert werden. Es sollte möglich sein, bereits während der Entwicklungsphase Maßnahmen zu berücksichtigen, die eine sichere Ausführung solcher Arbeiten gewährleisten. Wird die frühzeitige Realisierung versäumt, ist sie später vielleicht nur sehr schwer oder gar nicht mehr möglich. Daraus resultiert eventuell, dass die Justierung beweglicher Teile zwar dennoch vorgenommen werden muss, doch auf eine Weise, die entweder unsicher oder ineffizient (oder beides) ist. Eine Maschine, bei der alle Aufgaben während der Risikobeurteilung berücksichtigt werden, ist am Ende sicherer und effizienter.

Der Anwender (oder Arbeitgeber) muss sicherstellen, dass die Maschinen in ihrer Arbeitsumgebung sicher sind. Auch wenn eine Maschine vom Hersteller als sicher deklariert wurde, muss der Maschinenanwender dennoch eine Risikobeurteilung vornehmen, um bestimmen zu können, ob die Anlage in ihrer Umgebung sicher ist. Maschinen werden oft unter Bedingungen eingesetzt, die der Hersteller nicht berücksichtigt hat. Beispiel: Bei einer Fräsmaschine, die in einer Lehrwerkstatt eingesetzt wird, müssen mehr Faktoren berücksichtigt werden als bei einer Fräsmaschine, die in einer industriellen Fertigung verwendet wird.

Wenn ein Fertigungsbetrieb mehrere unabhängige Maschinen kauft und in einen Prozess integriert, ist der Fertigungsbetrieb der Hersteller der resultierenden kombinierten Maschine.

Im Folgenden werden die wesentlichen Schritte auf dem Weg zu einer zweckmäßigen Sicherheitsstrategie betrachtet. Die folgenden Ausführungen beziehen sich auf bestehende Werksinstallationen oder einzelne neue Maschinen.

Risikobeurteilung

Es ist falsch, die Risikobeurteilung als lästige Aufgabe zu betrachten. Eine Risikobeurteilung ist ein hilfreicher Prozess, der lebenswichtige Informationen liefert und den Nutzer oder Entwickler in die Lage versetzt, logische Entscheidungen über Wege zum Erreichen von Sicherheit zu treffen.

Zahlreiche Normen befassen sich mit diesem Thema. ISO 14121: „Grundsätze für die Risikobeurteilung“ und ISO 12100: „Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze“ enthalten die am häufigsten angewandten Leitlinien.

Unabhängig von der für die Risikobeurteilung verwendeten Technik erzielt ein Team mit Spezialisten der unterschiedlichsten Fachrichtungen ein ausgewogeneres Ergebnis mit einer größeren Abdeckung als eine Einzelperson.

Die Risikobeurteilung ist ein iterativer Prozess, der während der unterschiedlichsten Nutzungsphasen der Maschine ausgeführt werden kann. Die verfügbaren Informationen variieren abhängig von der jeweiligen Nutzungsphase. Beispielsweise bietet eine Risikobeurteilung durch einen Maschinenbauer Aufschluss über alle Details des Maschinenmechanismus und der Konstruktionsmaterialien, doch eventuell nur eine vage Einschätzung der letztendlichen Arbeitsumgebung der Maschine. Eine Risikobeurteilung, die durch den Maschinenanwender durchgeführt wird, gibt nicht unbedingt Aufschluss über präzise technische Details, informiert jedoch über alle Details der Arbeitsumgebung. Optimalerweise wird das Ergebnis einer Iteration auch gleich bei der nächsten Iteration einbezogen.

Bestimmung von Maschinengrenzen

Hierzu gehört das Sammeln und Analysieren von Informationen zu Teilen, Mechanismen und Funktionen einer Maschine. Außerdem müssen alle Typen menschlicher Interaktionen mit der Maschine und die Umgebung, in der die Maschine eingesetzt wird, berücksichtigt werden. Ziel ist es, die Maschine und ihre Verwendung eindeutig zu verstehen.

Wo separate Maschinen miteinander verkettet sind, entweder mechanisch oder durch Steuerungssysteme, sind diese als einzelne Maschinen zu betrachten, sofern sie nicht durch entsprechende Schutzmaßnahmen in Zonen unterteilt wurden.

Es ist wichtig, alle Grenzen und Phasen der Nutzungsdauer einer Maschine zu berücksichtigen. Hierzu zählen Montage, Inbetriebnahme, Instandhaltung, Stilllegung, bestimmungsgemäßer Gebrauch und Betrieb sowie die Folgen offensichtlicher Fehlverwendung oder Fehlfunktionen.

Erkennung von Aufgaben und Gefahren

Alle Gefahren an der Maschine müssen identifiziert und nach Art und Position geordnet aufgelistet werden. Zu den Gefahren zählen Quetschen, Scheren, Einziehen, Aufwickeln, Werkstückauswurf, Rauchgase, Strahlung, giftige Substanzen, Hitze, Lärm usw.

Die Ergebnisse der Aufgabenanalyse müssen mit den Ergebnissen der Gefahrenidentifikation verglichen werden. So zeigt sich, wo eine Gefahr und eine Person aufeinander treffen können, d. h. wo eine gefährliche Situation entstehen kann. Alle gefährlichen Situationen müssen aufgelistet werden. Eventuell kann dieselbe Gefahr zu unterschiedlichen gefährlichen Situationen führen (abhängig von der Natur der Person oder der Aufgabe). Beispielsweise kann die Anwesenheit eines hoch qualifizierten und geschulten Kundendiensttechnikers andere Auswirkungen haben als die Anwesenheit einer unqualifizierten Reinigungskraft, die mit der Maschine nicht vertraut ist. Wird in einer solchen Situation jeder Fall aufgelistet und separat angegangen, können eventuell unterschiedliche Schutzmaßnahmen für den Kundendiensttechniker und die Reinigungskraft gerechtfertigt werden. Werden die Fälle nicht separat aufgelistet und angegangen, muss vom schlimmsten Fall ausgegangen werden, d. h. für Kundendiensttechniker und Reinigungskraft werden dieselben Schutzmaßnahmen festgelegt.

Manchmal muss eine allgemeine Risikobeurteilung an einer vorhandenen Maschine vorgenommen werden, an der bereits Schutzmaßnahmen angebracht wurden (z. B. eine Maschine mit gefährlichen beweglichen Teilen, die durch eine Schutzgitterverriegelung geschützt sind). Die gefährlichen beweglichen Teile stellen eine potenzielle Gefahr dar, die zu einer direkten Gefahr werden kann, falls das Verriegelungssystem versagen sollte. Solange dieses Verriegelungssystem noch nicht validiert wurde (z. B. durch eine Risikobeurteilung oder durch eine mit einer Norm konformen Konstruktion), darf es nicht berücksichtigt werden.

Risikoabschätzung

Dies ist der fundamentalste Aspekt der Risikobeurteilung. Dieses Thema kann auf unterschiedliche Weisen angegangen werden. Auf den folgenden Seiten werden die grundlegenden Prinzipien dargelegt.

Alle Maschinen mit möglichen Gefahrenquellen bergen das Risiko eines gefährlichen Ereignisses (also eines Schadens). Je größer das Risiko, desto wichtiger wird es, etwas dagegen zu tun. Bei der einen Gefahr kann das Risiko so klein sein, dass es toleriert und akzeptiert werden mag. Doch bei einer anderen Gefahr ist das Risiko eventuell so groß, dass extreme Schutzmaßnahmen erforderlich werden. Damit eine Entscheidung getroffen werden kann, „ob und was gegen das Risiko zu tun ist“, muss es sich quantifizieren lassen.

Ein Risiko wird oft nur nach dem bewertet, wie schwer bei einem Unfall eine Verletzung sein kann. Doch es muss nicht nur die Schwere der potenziellen Verletzung berücksichtigt werden, sondern AUCH die Wahrscheinlichkeit ihres Auftretens, um die Höhe des vorhandenen Risikos abzuschätzen.

Die auf den folgenden Seiten gegebenen Ratschläge zur Risikoabschätzung haben lediglich Empfehlungscharakter, da sowohl das letztendlich gewählte Verfahren als auch die individuellen Umstände möglicherweise eine andere Vorgehensweise erforderlich machen. ES HANDELT SICH LEDIGLICH UM EINE ALLGEMEINE RICHTLINIE ZUR FÖRDERUNG EINER SYSTEMATISCHEN UND DOKUMENTIERTEN VORGEHENSWEISE.

Das verwendete Punktesystem wurde für keinen bestimmten Anwendungstyp ausgelegt und eignet sich daher eventuell für einige Anwendungen nicht. ISO TR (Technical Report) 14121-2 „Risikobeurteilung – Praktische Anleitung und Verfahrensbeispiele“ stellt praxisbezogene Anweisungen zur Verfügung und erläutert verschiedene Methoden zur Quantifizierung von Risiken.

Es werden folgende Faktoren berücksichtigt:

- SCHWERE DER POTENZIELLEN VERLETZUNG.
- WAHRSCHEINLICHKEIT IHRES AUFTRETENS.

Die Wahrscheinlichkeit des Auftretens unterliegt zwei Faktoren:

- HÄUFIGKEIT DES AUFENTHALTS IM GEFAHRENBEREICH.
- WAHRSCHEINLICHKEIT EINER VERLETZUNG.

Als Ergebnis einer unabhängigen Betrachtung jedes Faktors werden diesen Faktoren die entsprechenden Werte zugeordnet.

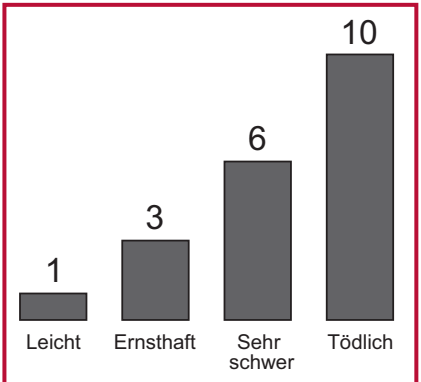
Verwerten Sie Daten und Erfahrungswerte, die Ihnen zur Verfügung stehen. Es werden alle Nutzungsphasen einer Maschine behandelt. Um eine unnötige Komplexität zu vermeiden, gründen Sie Ihre Entscheidungen also auf den ungünstigsten Fall für jeden Faktor.

Außerdem ist es wichtig, stets vernünftig zu handeln. Bei den Entscheidungen muss berücksichtigt werden, was durchführbar, realistisch und plausibel ist. Und genau deshalb ist das Konzept eines Teams mit Spezialisten der unterschiedlichsten Fachrichtungen so wertvoll.

Denken Sie daran, dass Sie zum Zwecke dieser Übung in der Regel nicht davon ausgehen, dass bereits ein Schutzsystem vorhanden ist. Falls diese Risikoabschätzung zeigt, dass ein Schutzsystem erforderlich ist, folgen weiter hinten in diesem Kapitel einige Anweisungen, mit deren Hilfe die erforderlichen Merkmale der Schutzeinrichtung bestimmt werden können.

1. Schwere der potenziellen Verletzung

Für diese Betrachtung wird davon ausgegangen, dass ein Unfall oder Störfall aufgetreten ist, z. B. als Folge der Gefahr. Eine sorgfältige Untersuchung der Gefahr ergibt die schwerstmögliche Verletzung. Denken Sie daran: Hier wird davon ausgegangen, dass eine Verletzung unvermeidbar ist und es nur darum geht, die Schwere der Verletzung zu bewerten. Es ist davon auszugehen, dass der Bediener mit der gefährlichen Bewegung oder dem gefährlichen Prozess in Berührung kommt. Die Schwere einer Verletzung wird eingestuft als:



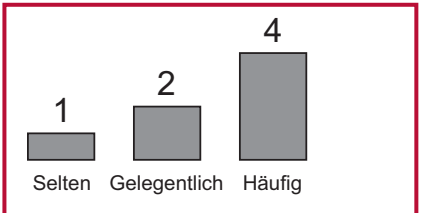
Der Schwere zugeordnete Punkte

- TÖDLICH: Tod
- SEHR SCHWER: (normalerweise irreversibel) Dauerhafte Behinderung, Verlust des Augenlichts, Amputation von Gliedmaßen, Schädigung der Atemwege usw.
- ERNSTHAFT: (normalerweise reversibel, d. h. ohne bleibende Schädigung) Bewusstlosigkeit, Verbrennungen, Brüche usw.
- LEICHT: Prellungen, Schnitte, leichte Abschürfungen usw.

Jeder Beschreibung wird einer der dargestellten Punktwerte zugeordnet.

2. Häufigkeit des Aufenthalts im Gefahrenbereich

Die Häufigkeit des Aufenthalts im Gefahrenbereich gibt Aufschluss darüber, wie oft der Bediener oder der Kundendiensttechniker der Gefahr ausgesetzt ist. Die Häufigkeit des Aufenthalts im Gefahrenbereich lässt sich wie folgt klassifizieren:



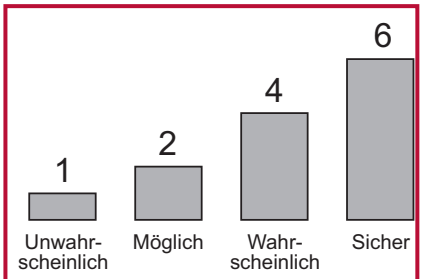
Der Häufigkeit des Aufenthalts im Gefahrenbereich zugeordnete Punkte

- HÄUFIG: mehrmals täglich
- GELEGENTLICH: täglich
- SELTEN: wöchentlich oder noch seltener

Jeder Beschreibung wird einer der dargestellten Punktwerte zugeordnet.

3. Wahrscheinlichkeit einer Verletzung

Es ist davon auszugehen, dass der Bediener mit der gefährlichen Bewegung oder dem gefährlichen Prozess in Berührung kommt. Durch Betrachten der Interaktion zwischen Bediener und Maschine und anderer Faktoren (z. B. Anlaufgeschwindigkeit) kann die Wahrscheinlichkeit einer Verletzung wie folgt klassifiziert werden:



Der Häufigkeit des Aufenthalts im Gefahrenbereich zugeordnete Punkte

- UNWAHRSCHEINLICH
- WAHRSCHEINLICH
- MÖGLICH
- SICHER

Jeder Beschreibung wird einer der dargestellten Punktwerte zugeordnet.

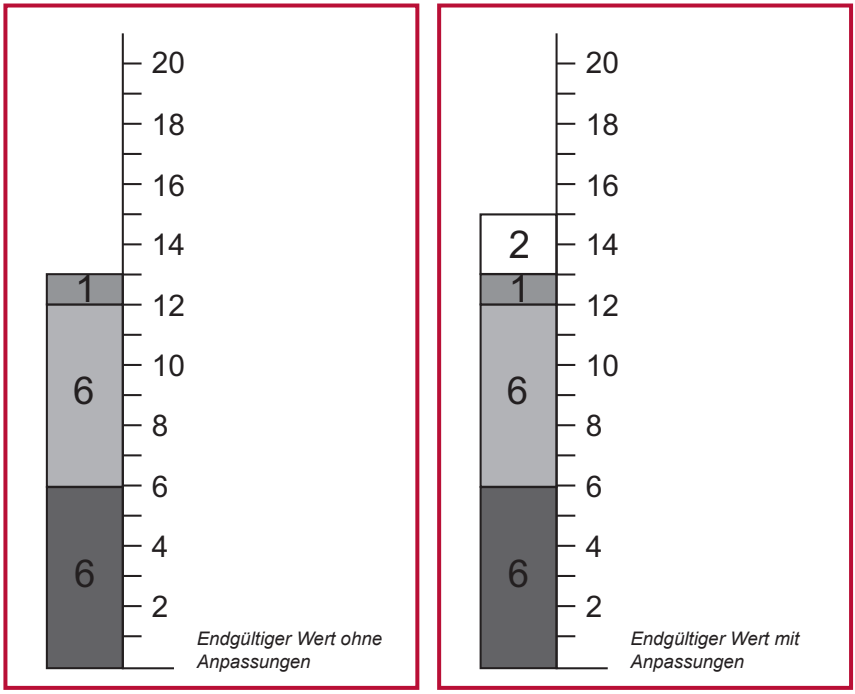
Allen Wahrscheinlichkeiten wird ein Wert zugeordnet; die addierten Werte ergeben einen ersten Schätzwert. Die Summe der drei Komponenten wird zu einem Wert von 13 addiert. Doch es sind einige weitere Faktoren zu berücksichtigen. (Hinweis: Dies basiert nicht unbedingt auf den Bildern des vorherigen Beispiels.)

Im nächsten Schritt wird die erste Schätzung angepasst, indem zusätzliche Faktoren berücksichtigt werden, wie z. B. die Faktoren in der folgenden Tabelle. Oft ist eine richtige Einstufung erst möglich, wenn die Maschine an ihrem endgültigen Standort installiert ist.

Typischer Faktor	**Empfohlene Aktion**
Mehrere Personen sind der Gefahr ausgesetzt	Multiplizieren des Schwerefaktors mit der Anzahl der Personen
Längere Zeit in der Gefahrenzone ohne vollständige Potenzialtrennung	Dauert der einzelne Zugriff länger als 15 Minuten, 1 Punkt zum Häufigkeitsfaktor addieren
Bediener ist unqualifiziert oder ungeschult	Zum Gesamtergebnis 2 Punkte addieren
Sehr lange Intervalle (z. B. 1 Jahr) zwischen Zugriffen. (Fehler können sich über längere Zeit entwickeln und unerkannt bleiben, besonders in Überwachungssystemen.)	Eine dem größten Häufigkeitsfaktor entsprechende Punktzahl addieren

Zusätzliche Überlegungen für die Risikoabschätzung

Die Ergebnisse zusätzlicher Faktoren werden zu der vorher ermittelten Summe addiert.



Risikominderung

Nun muss erneut jede Maschine mit ihren jeweiligen Risiken betrachtet werden, damit Maßnahmen gegen alle Gefahren ergriffen werden können.

Die folgende Tabelle zeigt einen dokumentierten Prozess zum Bewerten sämtlicher Sicherheitsaspekte der eingesetzten Maschinen. Es handelt sich um einen Leitfaden für Maschinennutzer, doch auch Hersteller oder Lieferanten von Maschinen können das gleiche Prinzip anwenden, um nachzuweisen, dass alle Arbeitsmittel bewertet wurden. Die Tabelle dient auch als Index für ausführlichere Berichte zur Risikobeurteilung.

Aus den Daten geht hervor, dass eine Maschine, die das CE-Zeichen trägt, den Prozess vereinfacht, da bereits der Hersteller die Maschinengefahren bewertet und alle notwendigen Maßnahmen ergriffen hat. Selbst bei Maschinen, die das CE-Zeichen tragen, bestehen möglicherweise noch Gefahren, die durch die Art der Anwendung oder die verarbeiteten Materialien bedingt sind und die der Hersteller nicht vorausgesehen hat.

Unternehmen – MAYKIT WRIGHT LTD
Einrichtung – Werkzeugraum – Werk Ost
Datum – 29.08.95
Bedienerprofil – qualifiziert.

Anlagen-ID und Datum	Konformität mit Richtlinien	Risiko-beurteilung Berichts-nummer	Bisherige Unfälle	Hinweise	Gefahren-identität	Gefahrentyp	Erforderliche Maßnahmen	Implementiert und überprüft – Referenz
Bloggs-Spitzendrehbank. Seriennr. 8390726 Installiert 1978	Keine angefordert	RA302	Keine	Die elektrische Einrichtung ist konform mit BS EN 60204, Not-Aus-Schalter wurden angebracht (ersetzt 1989)	Rotation der Spannzange bei geöffneter Schutzvorrichtung	Verfangen in der Mechanik Schnittwunden	Anbringen eines Türverriegelungs-schalters	11/25/94 J Kershaw Bericht Nr. 9567
					Schneidflüssigkeit	Giftig	Verwenden nicht giftiger Substanzen	11/30/94 J Kershaw Bericht Nr. 9714
					Beseitigung von Spänen	Schnittwunden	Bereitstellen von Handschuhen	11/30/94 J Kershaw Bericht Nr. 9715
Bloggs-Revolver-kopffräsen m/c Seriennr. 17304294 Hergestellt 1995 Installiert im Mai 95	Maschinen-richtlinie EMV-Richtlinie	RA416	Keine		Bewegung des Betts (zur Wand hin)	Quetschungen	Maschine verschieben, um genügend Abstand zu gewährleisten	4/13/95 J Kershaw Bericht Nr. 10064

Maßnahmenhierarchie zur Ausschaltung von Risiken

Es gibt drei grundlegende Methoden, die in der folgenden Reihenfolge berücksichtigt und verwendet werden müssen:

1. Ausschalten oder Verringern des Risikos so weit wie möglich (eigensichere Konstruktion und eigensicherer Aufbau der Maschine)
2. Installieren der erforderlichen Schutzsysteme und -maßnahmen (z. B. Schutzgitter-verriegelung, Lichtgitter) abhängig von den Risiken, die durch die Konstruktion nicht eliminiert werden können
3. Informieren der Bediener über Restrisiken aufgrund von Defiziten der ergriffenen Schutzmaßnahmen, Definieren des Bedarfs an speziellen Schulungen und Vorschreiben der zu verwendenden persönlichen Schutzausrüstung

Jede Maßnahme der Schutzhierarchie muss von oben her in Erwägung gezogen und angewendet werden, wo es möglich ist. Dies führt in der Regel zu einer Kombination von Maßnahmen.

Eigensichere Konstruktion

Während der Entwicklungsphase der Maschine können viele der möglichen Gefahren allein dadurch vermieden werden, dass Faktoren wie Material, Zugangsanforderungen, heiße Oberflächen, Übertragungsverfahren, Störstellen, Spannungspegel usw. sorgfältig berücksichtigt werden.

Ist beispielsweise der Zugang zu einem Gefahrenbereich nicht erforderlich, besteht die Lösung darin, diesen Bereich innerhalb des Maschinenaufbaus zu schützen oder eine fest montierte und geschlossene Schutzeinrichtung anzubringen.

Schutzsysteme und -maßnahmen

Wenn der Zugang erforderlich ist, kann es etwas schwieriger sein, eine Lösung zu finden. Es muss sichergestellt werden, dass ein Zugang nur möglich ist, während sich die Maschine in einem sicheren Zustand befindet. Schutzmaßnahmen wie verriegelte Schutztüren und/oder Auslösesysteme sind erforderlich. Die Wahl der Schutzeinrichtung oder des Schutzsystems wird stark durch die Betriebseigenschaften der Maschine beeinflusst. Dies ist äußerst wichtig, denn ein Schutzsystem, das die Effizienz der Maschine beeinträchtigt, ist anfällig für Versuche, den Schutz zu entfernen oder zu umgehen.

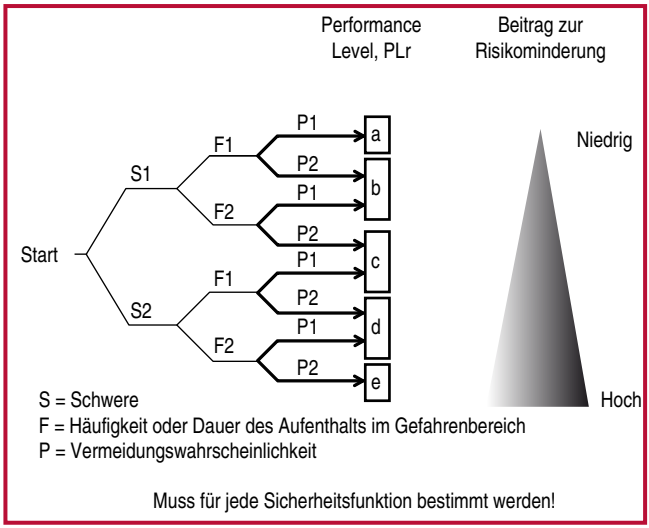
Die Sicherheit der Maschine hängt in diesem Fall vom richtigen Anbringen und der korrekten Funktion des Schutzsystems selbst unter Fehlerbedingungen ab.

Jetzt muss die korrekte Funktion des Systems betrachtet werden. Für jede Art von Schutzsystem besteht die Wahl zwischen Technologien mit unterschiedlicher Leistungsfähigkeit hinsichtlich der Überwachung, Erkennung und Vermeidung von Fehlern.

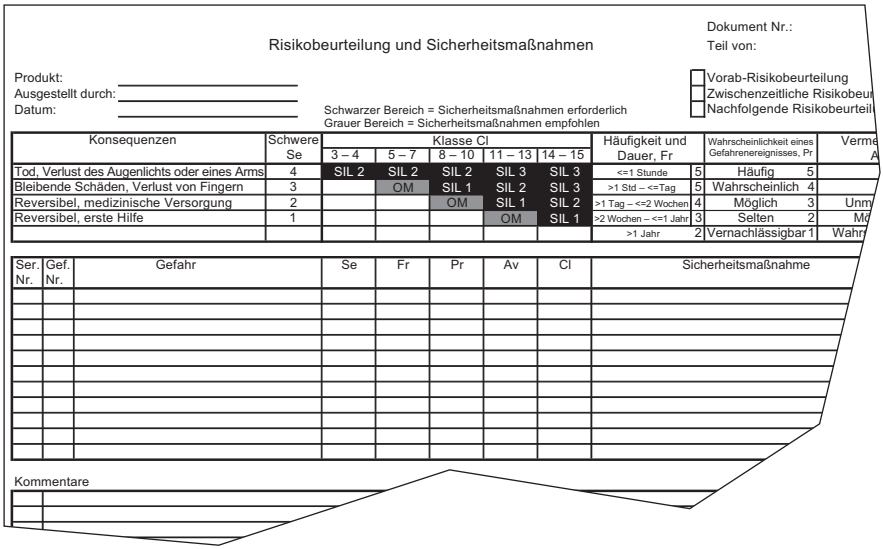
Im Idealfall wäre jedes Schutzsystem perfekt, absolut ausfallsicher und würde unter keinen Umständen zu gefährlichen Bedingungen führen. In Wirklichkeit gibt es jedoch Grenzen hinsichtlich des Know-hows und des Materials. Eine weitere, sehr reale Einschränkung sind die Kosten. Anhand dieser Faktoren wird offensichtlich, dass die Verhältnismäßigkeit gewahrt bleiben muss. Es wäre übertrieben, für eine Maschine, die im schlimmsten Fall leichte Hautabschürfungen verursacht, und für ein System, das ein Passagierflugzeug in der Luft hält, den gleichen Maßstab für die Integrität der Schutzsysteme anzulegen. Die Folgen eines Ausfalls wären sehr unterschiedlich, und deshalb muss es eine Möglichkeit geben, den Umfang der Schutzmaßnahmen mit der Höhe des im Rahmen der Risikoabschätzung ermittelten Risikos ins Verhältnis zu setzen.

Unabhängig von der ausgewählten Art der Schutzeinrichtung ist zu bedenken, dass ein „sicherheitsbezogenes System“ eine Vielzahl von Elementen umfassen kann, einschließlich Schutzeinrichtung, Verdrahtung, Leistungsschaltgerät und manchmal Teile des Steuerungssystems der Maschine. Alle Elemente des Systems (einschließlich Schutzvorrichtungen, Befestigung, Verdrahtung usw.) müssen geeignete Leistungsmerkmale hinsichtlich der Entwicklungsgrundsätze und Technologien aufweisen. IEC/EN 62061 und EN ISO 13849-1 klassifizieren hierarchische Leistungsebenen für sicherheitsbezogene Teile von Steuerungssystemen und bieten in ihren Anhängen Risikobeurteilungsmethoden zur Bestimmung der Integritätsanforderungen für ein Schutzsystem.

EN ISO 13849-1:2008 enthält in Anhang A ein erweitertes Risikodiagramm.



IEC 62061 beschreibt in Anhang A ebenfalls ein Verfahren, das in etwa wie folgt aussieht.



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil von:

Produkt:
Ausgestellt durch:
Datum:

Schwarzer Bereich = Sicherheitsmaßnahmen erforderlich
Grauer Bereich = Sicherheitsmaßnahmen empfohlen

☐ Vorab-Risikobeurteilung
☐ Zwischenzeitliche Risikobeur
☐ Nachfolgende Risikobeurteil

Konsequenzen	Schwere Se	Klasse Cl 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Häufigkeit und Dauer, Fr		Wahrscheinlichkeit eines Gefahrenereignisses, Pr		Verme A
Tod, Verlust des Augenlichts oder eines Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<=1 Stunde	5	Häufig	5	
Bleibende Schäden, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	>1 Std – <=Tag	5	Wahrscheinlich	4	
Reversibel, medizinische Versorgung	2			OM	SIL 1	SIL 2	>1 Tag – <=2 Wochen	4	Möglich	3	Unm
Reversibel, erste Hilfe	1				OM	SIL 1	>2 Wochen – <=1 Jahr	3	Selten	2	Mö
							>1 Jahr	2	Vernachlässigbar	1	Wahr

Ser. Nr.	Ges. Nr.	Gefahr	Se	Fr	Pr	Av	Cl	Sicherheitsmaßnahme

Kommentare

Die Verwendung einer der oben beschriebenen Verfahren sollte zu gleichwertigen Ergebnissen führen. Jedes Verfahren berücksichtigt den Inhalt der Norm, zu der es jeweils gehört.

In beiden Fällen ist es äußerst wichtig, dass die im Text der Norm enthaltenen Anleitungen befolgt werden. Risikodiagramm und Tabelle dürfen nicht isoliert oder auf zu einfache Weise verwendet werden.

Beurteilung

Nach dem Auswählen der Schutzmaßnahme und vor ihrer Realisierung muss die Risikoabschätzung unbedingt wiederholt werden. Dieses Verfahren wird häufig übergangen. Möglicherweise geht der Bediener der Maschine nach dem Installieren der Schutzmaßnahme davon aus, dass er vollständig und lückenlos vor dem ursprünglich als potenziell bestehend angenommenen Risiko geschützt ist. Da dem Bediener die ursprüngliche Gefahr nicht mehr in dem Maße bewusst ist wie zuvor, verhält er sich an der Maschine eventuell völlig anders. Dadurch wird er der Gefahr unter Umständen öfter ausgesetzt oder dringt beispielsweise weiter in die Maschine ein. Dies bedeutet, dass der Bediener bei einem Ausfall der Schutzmaßnahme einem größeren Risiko ausgesetzt ist als zuvor angenommen. Hierbei handelt es sich um das tatsächliche Risiko, das abgeschätzt werden muss. Daher muss die Risikoabschätzung wiederholt werden. Bei dieser Wiederholung sind alle vorhersehbaren Änderungen der Verhaltensweisen von Personen bei der Interaktion mit der Maschine zu berücksichtigen. Auf diese Weise wird überprüft, ob die vorgeschlagenen Schutzmaßnahmen tatsächlich geeignet sind. Weitere Informationen enthält Anhang A der Norm IEC/EN 62061.

Schulung, persönliche Schutzausrüstung usw.

Es ist wichtig, Bedienern sichere Arbeitsmethoden für eine Maschine durch Schulung zu vermitteln. Dies bedeutet nicht, dass die anderen Maßnahmen entfallen können. Es ist nicht akzeptabel, einem Bediener lediglich zu sagen, dass er sich gefährlichen Bereichen nicht nähern darf (als Alternative zum Schützen der gefährlichen Bereiche).

Eventuell ist es für den Bediener auch notwendig, Spezialhandschuhe, Schutzbrille, Atemschutz usw. zu verwenden. Der Maschinenentwickler muss angeben, welche Ausrüstung erforderlich ist. Die Verwendung persönlicher Schutzausrüstung stellt normalerweise nicht das Hauptschutzverfahren dar, ergänzt aber die oben beschriebenen Maßnahmen.

Normen

Viele Normen und technischen Berichte enthalten Anleitungen zur Risikobeurteilung. Einige wurden für ein breites Anwendungsgebiet verfasst, andere wiederum für spezielle Anwendungen. In der folgenden Liste sind Normen aufgeführt, die Informationen zur Risikobeurteilung umfassen.

ANSI B11.TR3: Informationen zur Risikobeurteilung und Risikominderung – Eine Anleitung zum Abschätzen, Beurteilen und Mindern von Risiken im Zusammenhang mit Werkzeugmaschinen

ANSI PMMI B155.1: Informationen zu sicherheitstechnischen Anforderungen für Verpackungsmaschinen und verpackungsbezogene Produktveredelungsmaschinen

ANSI RIA R15.06: Informationen zu sicherheitstechnischen Anforderungen für Industrieroboter und Robotersysteme

AS 4024.1301-2006: Informationen zu den Grundsätzen für die Risikobeurteilung
(CSA Z432-04): Informationen zum Schutz von Maschinen

CSA Z434-03: Informationen zu Industrierobotern und Robotersystemen – Allgemeine sicherheitstechnische Anforderungen

IEC/EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

IEC/EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen

EN ISO 14121-1: Leitsätze zur Risikobeurteilung

ISO TR 14121-2: Risikobeurteilung – Praktische Anleitung und Verfahrensbeispiele.

Schutzmaßnahmen und ergänzende Ausrüstung

Wenn die Risikobeurteilung zeigt, dass eine Maschine oder ein Prozess eine Verletzungsgefahr mit sich bringt, muss die Gefahr beseitigt oder begrenzt werden. Die Art und Weise, wie dies erreicht wird, hängt von der Beschaffenheit der Maschine und der Gefahr ab. Schutzmaßnahmen in Verbindung mit Schutzvorrichtungen verhindern entweder den Zugang zu einer Gefahr oder verhindern gefährliche Bewegungen an einer Gefahrenstelle, wenn der Zugang möglich ist. Typische Beispiele für Schutzmaßnahmen sind fest installierte Schutzvorrichtungen, Schutzgitterverriegelungen, Lichtgitter, Schaltmatten, 2-Hand-Bedienungen und Aktivierungsschalter.

Not-Halt-Geräte und -Systeme sind sicherheitsbezogenen Steuerungssystemen zugeordnet, stellen jedoch keine direkten Schutzsysteme dar. Sie dürfen lediglich als ergänzende Schutzmaßnahmen betrachtet werden.

Verhindern des Zugangs durch fest installierte, geschlossene Schutzvorrichtungen

Besteht die Gefahr in einem Maschinenteil, das nicht zugänglich sein muss, sollte eine Schutzeinrichtung fest an der Maschine installiert werden. Diese Art von Schutzeinrichtung kann nur mit Werkzeugen entfernt werden. Die fest installierten Schutzeinrichtungen müssen 1) ihrer Betriebsumgebung standhalten, 2) wo erforderlich, Projektile eindämmen und 3) keine Gefahrenquellen darstellen, z. B. durch scharfe Kanten. Fest installierte Schutzeinrichtungen können Öffnungen aufweisen, an denen die Schutzeinrichtung auf die Maschine trifft, oder Öffnungen, die dadurch entstehen, dass ein Drahtgittergehäuse verwendet wird.

Fenster sind eine praktische Möglichkeit, die Maschinenleistung zu überwachen, wenn Zugang zu diesem Teil der Maschine erforderlich ist. Dabei muss das verwendete Material mit Sorgfalt ausgewählt werden, da sich das Fenstermaterial mit der Zeit durch chemische Reaktionen mit Schneidflüssigkeiten, ultraviolette Strahlung und durch den normalen Alterungsprozess verschlechtern kann.

Die Öffnungen dürfen nur so groß sein, dass ein Bediener keinen Zugang zur Gefahrenquelle hat. Tabelle O-10 in U.S. OHSA 1910.217 (f) (4), ISO 13854, Tabelle D-1 von ANSI B11.19, Tabelle 3 in CSA Z432 und AS4024.1 enthalten Informationen dazu, wie weit eine Öffnung von der Gefahrenquelle entfernt sein muss.

Zugriffserkennung

Schutzmaßnahmen dienen dazu, den Zugang zu einer Gefahrenquelle zu erkennen. Wenn die Zugriffserkennung als Möglichkeit zur Risikominderung ausgewählt wird, muss der Entwickler verstehen, dass ein umfassendes Sicherheitssystem zu verwenden ist. Die Schutzeinrichtung selbst bietet nicht die erforderliche Risikominderung.

Dieses Sicherheitssystem besteht in der Regel aus drei Blöcken: 1) ein Eingangsgerät, das den Zugriff auf die Gefahrenquelle erkennt, 2) ein Logikgerät, das die Signale vom erkennenden Gerät verarbeitet, den Status des Sicherheitssystems überprüft und die Ausgangsgeräte ein- oder ausschaltet, und 3) ein Ausgangsgerät, das den Aktor (z. B. einen Motor) steuert.

Erkennungsgeräte

Zum Erkennen einer Person, die einen Gefahrenbereich betritt oder sich in einem solchen befindet, gibt es zahlreiche alternative Geräte. Die optimale Wahl für eine bestimmte Anwendung hängt von den unterschiedlichsten Faktoren ab.

- Häufigkeit des Zugangs,
- Zeit, die zum Ausschalten der Gefahrenquelle erforderlich ist,
- Wichtigkeit des Abschlusses eines Maschinenzyklus und
- Eindämmung von Projektilen, Flüssigkeiten, Dunst, Dämpfen usw.

Richtig ausgewählte bewegliche Schutzeinrichtungen können verriegelt werden, um Schutz vor Projektilen, Flüssigkeiten, Dämpfen und anderen Gefahrentypen zu bieten. Sie werden häufig eingesetzt, wenn der Zugriff auf die Gefahrenquelle selten erfolgt. Verriegelte Schutzeinrichtungen können auch verriegelt werden, um den Zugriff zu verhindern, während sich die Maschine mitten in einem Zyklus befindet und wenn die Maschine bis zum endgültigen Stopp lange Zeit benötigt.

Sicherheitsgeräte mit Annäherungsfunktion wie Lichtgitter, Schaltmatten und Scanner bieten einen schnellen und einfachen Zugang zum Gefahrenbereich und werden oft eingesetzt, wenn die Bediener häufigen Zugang zum Gefahrenbereich benötigen. Diese Gerätetypen bieten keinen Schutz vor Projektilen, Dämpfen, Flüssigkeiten und anderen Gefahrentypen.

Die beste Schutzmaßnahme ist die Wahl eines Geräts oder Systems, das maximale Schutzwirkung bei minimaler Behinderung des normalen Maschinenbetriebs bietet. Es müssen alles Aspekte der Maschine berücksichtigt werden, da die Erfahrung zeigt, dass ein schwierig zu benutzendes System eher entfernt oder umgangen wird.

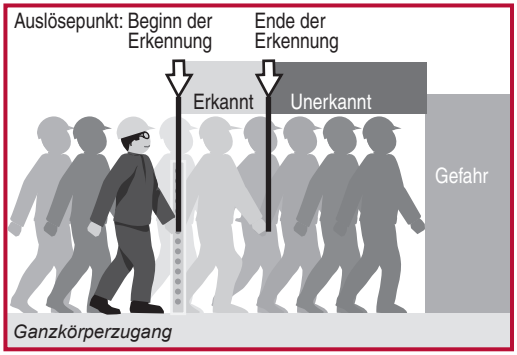
Sicherheitsgeräte mit Annäherungsfunktion

Bei der Entscheidung, wie ein Gefahrenbereich geschützt werden soll, muss genau bekannt sein, welche Sicherheitsfunktionen erforderlich sind. Dies sind normalerweise mindestens zwei Funktionen.

- Ausschalten oder Deaktivieren des Maschinenantriebs, wenn eine Person den Gefahrenbereich betritt.
- Verhindern des Einschaltens oder Aktivierens des Maschinenantriebs, wenn sich eine Person im Gefahrenbereich befindet.

Auf den ersten Blick scheinen diese Funktionen identisch zu sein. Tatsächlich handelt es sich aber um zwei verschiedene Funktionen, obwohl sie offensichtlich miteinander verknüpft sind

und oft durch die gleichen Geräte erreicht werden. Zum Erreichen der ersten Funktion wird eine Auslösevorrichtung benötigt. Damit ist ein Gerät gemeint, das erkennt, wenn ein Teil einer Person einen bestimmten Punkt überschreitet und ein Signal zum Ausschalten des Maschinenantriebs auslöst. Kann die Person über diesen Auslösepunkt hinaus weiter vordringen, während ihre Anwesenheit nicht mehr erkannt wird, gilt die zweite Funktion (Verhindern des Einschaltens) als nicht erreicht.



Die folgende Abbildung zeigt ein Beispiel für einen Ganzkörperzugang mit einem vertikal montierten Lichtgitter als Auslösevorrichtung. Schutzgitterverriegelungen können auch ausschließlich als Auslösungsgerät verwendet werden, wenn durch nichts verhindert wird, dass sich die Tür nach dem Eintreten schließt.

Ist kein Ganzkörperzugang möglich, sodass eine Person nicht über den Auslösepunkt hinaus gelangen kann, wird ihre Anwesenheit immer erkannt, und die zweite Funktion (Verhindern des Einschaltens) ist erreicht.

Bei Teilkörperanwendungen werden das Auslösen und das Erkennen der Anwesenheit von den gleichen Geräten übernommen. Der einzige Unterschied besteht in der Art der Anwendung.

Sicherheitsgeräte mit Annäherungsfunktion werden zum Erkennen des Vorhandenseins von Personen eingesetzt. Diese Gerätefamilie umfasst auch Sicherheitslichtgitter, Einweg-Sicherheitsbarrieren, Sicherheitsbereichsscanner, Schaltmatten und Schaltleisten.

Sicherheitslichtgitter

Sicherheitslichtgitter lassen sich als fotoelektrische Anwesenheitssensoren bezeichnen, die so gestaltet sind, dass Personal vor Verletzung durch gefährliche Maschinenbewegungen geschützt wird. Als sogenannte aktive optoelektronische Schutzeinrichtungen (AOPD) oder elektrosensitive Schutzausrüstung (ESPE) bieten Lichtgitter optimale Sicherheit bei höherer Produktivität. Sie stellen eine ergonomisch günstigere Lösung dar als mechanische Schutzvorrichtungen. Sie sind ideal geeignet für Anwendungen, in denen Personen häufig und problemlos Zugang zu einem bestimmten Betriebspunkt einer gefährlichen Maschine haben müssen.

Lichtgitter erfüllen die Anforderungen der Normen IEC 61496-1 und -2 und wurden entsprechend getestet. Es gibt keine harmonisierte EN-Version von Teil 2, sodass laut Anhang IV der europäischen Maschinenrichtlinie eine Zertifizierung der Lichtgitter durch Dritte erforderlich ist, bevor diese in der europäischen Union auf den Markt gebracht werden dürfen. Die Tests Dritter sorgen dafür, dass die Lichtgitter diese internationale Norm erfüllen. Underwriter's Laboratory hat die Norm IEC 61496-1 als US-Norm übernommen.

Sicherheitslaserscanner

Sicherheitslaserscanner verwenden einen rotierenden Spiegel, der Lichtimpulse über einen Bogen umlenkt und so eine Erkennungsebene erzeugt. Die Position des Objekts wird durch den Drehwinkel des Spiegels erkannt. Durch die Verwendung der „Flugzeit"-Technik eines reflektierten, unsichtbaren Lichtstrahls kann der Scanner auch erkennen, wie weit das Objekt vom Scanner entfernt ist. Mithilfe der gemessenen Entfernung und des Winkels bestimmt der Laserscanner die exakte Position des Objekts.

Sicherheitsschaltmatte

Diese Geräte dienen zum Überwachen eines Fußbodenbereichs um eine Maschine. Auf dem Fußboden im Gefahrenbereich werden Schaltmatten verlegt. Auf die Matte angewandter Druck (z. B. beim Betreten durch einen Bediener) bewirkt, dass das Mattensteuergerät die Energiezufuhr der gefährlichen Maschine abschaltet. Druckempfindliche Matten werden oft in geschlossenen Bereichen mit mehreren Maschinen verwendet, z. B. in flexiblen Fertigungsinseln oder Roboterzellen. Wenn Zugang zur Zelle erforderlich ist (z. B. zum Einlernen des Roboters), verhindern die Matten gefährliche Bewegungen, falls der Bediener den sicheren Bereich verlässt oder wenn er hinter ein Anlagenteil gelangen muss.

Bei der Dimensionierung und Positionierung der Matte muss der Sicherheitsabstand berücksichtigt werden.

Sicherheitsschaltleisten

Diese flexiblen Schaltleisten können an der Kante eines beweglichen Teils montiert werden, z. B. an einem Maschinentisch oder einem elektrischen Rolltor, um der Gefahr des Einklemmens oder Abscherens zu begegnen.

Falls das bewegliche Teil auf den Bediener trifft (oder umgekehrt), wird die Schaltleiste eingedrückt und gibt einen Befehl zum Ausschalten des Antriebs des gefährlichen Teils aus. Schaltleisten können auch zum Schutz an Maschinen eingesetzt werden, wenn die Gefahr besteht, dass der Bediener von beweglichen oder rotierenden Teilen erfasst wird. Verfängt sich ein Bediener in der Maschine, bewirkt der Kontakt mit der Schaltleiste das Stillsetzen des Maschinenantriebs.

Verschiedene Technologien können zum Erstellen von Schaltleisten eingesetzt werden. Eine gängige Technologie ist das Einfügen eines langen Schalters in die Leiste. Bei diesem Ansatz entstehen gerade Kanten, wobei in der Regel die 4-adrige Anschlusstechnik verwendet wird.

Lichtgitter, Scanner, Schaltmatten und Schaltleisten können als „Auslösevorrichtungen" klassifiziert werden. Diese Geräte können Annäherungen an gefährliche Bereiche nicht verhindern, sondern nur erkennen. Sie sind ausschließlich auf ihre Fähigkeit angewiesen, zum Zweck der Sicherheit sowohl zu erkennen als auch zu schalten: Im Allgemeinen sind sie nur sinnvoll an Maschinen, die nach dem Abschalten der Antriebsenergie ausreichend schnell zum Stillstand kommen. Da ein Bediener den Gefahrenbereich direkt betreten oder erreichen kann, muss die zum Anhalten der Bewegung notwendige Zeit kürzer sein als die Zeit, die der Bediener nach Auslösen des Geräts zum Erreichen der Gefahr benötigt.

Sicherheitsschalter

Ist der Zugang zur Maschine nur selten erforderlich, werden bewegliche (bedienbare) Schutzvorrichtungen bevorzugt. Die Schutzvorrichtung ist mit der Energiezufuhr der gefährlichen Maschine in einer Weise sicherheitsverriegelt, dass beim Öffnen der Schutztür die Energieversorgung abgeschaltet wird. Dieses Konzept umfasst die Verwendung eines Sicherheitsschalters, der an der Schutztür angebracht ist. Das Aus- und Wiedereinschalten der Energiezufuhr der gefährlichen Maschine erfolgt durch die Schaltsektion der Maschine. Die Energiequelle ist normalerweise elektrischer Strom, doch es kann sich auch um Druckluft oder Hydraulikdruck handeln. Wenn die Bewegung (Öffnung) der Schutztür erkannt wird, gibt der Sicherheitsschalter einen Befehl zum Trennen der Energiezufuhr der gefährlichen Maschine entweder direkt oder über ein Leistungsschütz (bzw. Ventil) aus.

Manche Sicherheitsschalter besitzen auch eine Sperre, die die Schutztür geschlossen hält und erst dann freigibt, wenn sich die Maschine in einem sicheren Zustand befindet. Für die meisten Anwendungsfälle ist die Kombination aus beweglicher Schutzvorrichtung und Sicherheitsschalter mit oder ohne Zuhaltung die zuverlässigste und kostengünstigste Lösung.

Eine Vielzahl von Sicherheitsschaltern steht zur Verfügung, wie etwa:

- **Sicherheitsschalter** – Bei diesen Geräten muss ein länglicher Betätiger in den Schalter eingeführt und herausgenommen werden, damit die Funktion ausgeführt wird.
- **Scharnierschalter** – Diese Geräte werden auf dem Scharnierstift einer Sicherheitstür angebracht und bei der Öffnungsaktion der Tür angesteuert.
- **Sicherheitszuhaltung** – Bei einigen Anwendungen muss die geschlossene Schutztür verriegelt oder das Öffnen der Schutztür verzögert werden. Für diese Anforderungen geeignete Geräte werden Sicherheitszuhaltungen genannt. Sie eignen sich für Maschinen, die durch eine längere Auslaufphase nach dem Abschalten gekennzeichnet sind, können aber auch eine deutliche Erhöhung des Schutzgrads für die meisten Maschinentypen bieten.

- **Berührungslose Sicherheitsschalter** – Diese Geräte erfordern keinen physischen Kontakt zur Betätigung. Einige Versionen sind darüber hinaus mit einer Codierungsfunktion ausgestattet, um einen besseren Schutz vor dem Zugriff unbefugter Personen zu gewährleisten.
- **Positionsschalter** – Die nockenbetätigte Auslösung findet meist mithilfe eines positiven Grenzschalters (oder Positionsschalters) und einer linearen oder rotierenden Nocke statt. Sie wird in der Regel bei Schiebeschutzvorrichtungen angewandt.
- **Schlüsseltransfersysteme** – Arretierte Schlüssel können die Steuerung und die Spannungsversorgung verriegeln. Bei der „Steuerungsverriegelung" gibt ein Verriegelungsgerät einen Stoppbefehl an ein zwischengeschaltetes Gerät aus, das ein nachfolgendes Gerät ausschaltet, um die Energie zum Aktor zu unterbrechen. Bei der „Verriegelung der Spannungsversorgung" unterbricht der Stoppbefehl die Energieversorgung zu den Maschinenaktoren direkt.

Bedienerschnittstellen-Geräte

Stoppfunktion – In den USA, Kanada und Europa sowie auf internationaler Ebene gibt es eine Harmonisierung der Normen hinsichtlich der Beschreibungen der Ausschaltkategorien für Maschinen oder Fertigungssysteme.

Hinweis: Diese Kategorien unterscheiden sich von den Kategorien der Norm EN 954-1 (ISO 13849-1). Näheres hierzu enthalten die Normen NFPA 79 und IEC/EN 60204-1. Ausschaltvorrichtungen sind in drei Kategorien unterteilt:

Kategorie 0 ist Stillsetzen durch sofortiges Abschalten der Maschinenantriebe. Dies wird als unkontrolliertes Stillsetzen bezeichnet. Bei abgeschalteter Antriebsenergie sind auf Antriebskraft angewiesene Bremsvorrichtungen ohne Wirkung. Deshalb können Motoren frei drehen und über einen längeren Zeitraum bis zum Stillstand auslaufen. In anderen Fällen können Werkstücke aus den auf Antriebskraft angewiesenen Haltevorrichtungen einer Maschine fallen. Mechanische Anhaltevorrichtungen, die keine Antriebskraft erfordern, können ebenfalls mit einer Ausschaltvorrichtung der Kategorie 0 eingesetzt werden. Ausschaltvorrichtungen der Kategorie 0 haben Priorität vor Ausschaltvorrichtungen der Kategorie 1 oder Kategorie 2.

Kategorie 1 ist gesteuertes Stillsetzen, wobei Energie zum Abbremsen und Anhalten der Maschinenantriebe verfügbar ist. Sobald die Maschine zum Stillstand gekommen ist, wird die Antriebsenergie abgeschaltet. Ausschaltvorrichtungen dieser Kategorie ermöglichen kraftunterstütztes Bremsen, um gefährliche Bewegungen schnell zu stoppen. Danach kann die Antriebsenergie abgeschaltet werden.

Kategorie 2 ist kontrolliertes Anhalten, wobei Energie für die Maschinenantriebe verfügbar bleibt. Ein normales Anhalten der Fertigung wird als Ausschaltvorgang der Kategorie 2 betrachtet.

Diese Ausschaltkategorien müssen auf jede Ausschaltfunktion angewendet werden, wobei die Ausschaltfunktion auf der Wirkung der sicherheitsbezogenen Teile eines Steuerungssystems bei Eingang eines Signals der Kategorie 0 oder 1 beruht. Ausschaltfunktionen

müssen entsprechende Einschaltfunktionen übersteuern. Die erforderliche Ausschaltkategorie für die jeweilige Ausschaltfunktion muss durch eine Risikobeurteilung bestimmt werden.

Not-Halt-Funktion

Die Not-Halt-Funktion muss als Ausschaltfunktion der Kategorie 0 oder 1 arbeiten, je nach Ergebnis der Risikobeurteilung. Sie muss durch eine einzige Handlung einer Person ausgelöst werden. Alle anderen Funktionen und Betriebsarten der Maschine bleiben dabei unberücksichtigt. Ziel ist es, den Antrieb so schnell wie möglich auszuschalten, ohne dass zusätzliche Gefahren entstehen.

Bis vor kurzem waren für Not-Halt-Stromkreise festverdrahtete elektromechanische Komponenten erforderlich. Jüngste Änderungen an Normen, wie z. B. IEC 60204-1 und NFPA 79, bedeuten, dass Sicherheits-SPS und andere Formen elektronischer Logik, die die Anforderungen von Normen wie z. B. IEC 61508 erfüllen, in Not-Halt-Stromkreisen verwendet werden können.

Not-Halt-Geräte

Überall dort, wo ein Bediener durch eine Maschine gefährdet werden kann, muss eine Einrichtung vorhanden sein, die den schnellen Zugriff auf ein Not-Halt-Gerät ermöglicht. Das Not-Halt-Gerät muss ständig betriebsfähig und ungehindert erreichbar sein. Bedienerschalttafeln müssen mindestens ein Not-Halt-Gerät enthalten. Zusätzliche Not-Halt-Geräte können nach Bedarf an anderen Stellen angeordnet werden. Not-Halt-Geräte sind in verschiedenen Formen erhältlich. Drucktastschalter und Seilzugschalter sind Beispiele für die gebräuchlichsten Gerätetypen. Wenn das Not-Halt-Gerät betätigt wird, muss es fest einrasten. Es darf nicht möglich sein, den Stoppbefehl ohne Selbsthaltung zu erzeugen. Die Rückstellung des Not-Halt-Geräts darf keine gefährliche Situation hervorrufen. Ein Wiederanlauf der Maschine darf nur durch eine separate und beabsichtigte Handlung möglich sein.

Weitere Informationen über Not-Halt-Geräte enthalten die Normen ISO/EN 13850, IEC 60947-5-5, NFPA 79 und IEC 60204-1, AS4024.1, Z432-94.

Not-Halt-Taster

Not-Halt-Geräte gelten als ergänzende Schutzeinrichtung. Sie sind keine primären Schutzeinrichtungen, da sie weder den Zugang zu einer Gefahrenquelle verhindern noch den Zugang zu einer Gefahrenquelle erkennen.

Normalerweise handelt es sich bei diesen Einrichtungen um einen roten Pilzkopftaster auf gelbem Hintergrund, den der Bediener im Notfall drückt. Die Anordnung der Not-Halt-Taster muss strategisch geplant werden. In der Umgebung der Maschine müssen genügend Not-Halt-Taster vorhanden sein, um sicherzustellen, dass an Gefahrenstellen immer ein Taster erreichbar ist.

Auf Not-Halt-Taster muss stets zugegriffen werden können. Außerdem müssen sie in allen Maschinenbetriebsarten verfügbar sein. Wenn eine Drucktaste als Not-Halt-Gerät verwendet wird, muss es sich dabei um einen pilzförmigen (oder mit der Handfläche bedienbaren), roten Schalter mit gelbem Hintergrund handeln. Beim Drücken der Drucktaste müssen die Kontakte den Zustand in dem Moment wechseln, wenn der Taster die gedrückte Position erreicht.

Eine der neuesten Technologien für Not-Halt-Taster ist die Selbstüberwachungstechnik. Auf der Rückseite des Not-Halt-Tasters wird ein zusätzlicher Kontakt angebracht, der überwacht, ob die Rückseite der Schalttafelkomponenten noch immer vorhanden ist. Dies wird auch als Kontaktblock mit Selbstüberwachung bezeichnet. Er besteht aus einem federbetätigten Kontakt, der schließt, wenn der Kontaktblock in seiner Position auf der Schalttafel einrastet. Abbildung 80 zeigt den Selbstüberwachungskontakt, der mit einem der direkt öffnenden Sicherheitskontakte in Reihe geschaltet ist.

Seilzugschalter

Bei Produktionsbändern ist es oft sinnvoller und effektiver, im Gefahrenbereich einen Seilzug als Not-Halt-Gerät vorzusehen. Diese Geräte bestehen aus einem Stahlseil, das mit selbsthaltenden Zugschaltern verbunden ist, so dass Ziehen am Seil in beliebiger Richtung und an beliebiger Stelle auf der gesamten Länge die Schalter auslöst und die Stromversorgung der Maschine trennt.

Die Seilzugschalter müssen einen Zug auf den Kabeln ebenso erkennen wie einen Durchhang. Das Erkennen von Durchhängen gewährleistet, dass das Kabel nicht durchtrennt wird und stets einsatzbereit ist.

Die Kabelabstände wirken sich auf die Leistung des Schalters aus. Bei kürzeren Abständen wird der Sicherheitsschalter an einem Ende montiert, während am anderen Ende eine Spannfeder angebracht wird. Bei längeren Abständen muss ein Sicherheitsschalter an beiden Kabelenden montiert werden, um sicherzustellen, dass eine einzige Aktion des Bedieners zum Ausgeben eines Stoppbefehls führt. Das Seil darf die Kraft von 200 N oder eine Entfernung von 400 mm an einer Position in der Mitte zwischen zwei Kabelhaltern nicht überschreiten.

2-Hand-Bedienung

Die Verwendung von 2-Hand-Bedienungen (auch als Zweihandschaltung bezeichnet) ist ein übliches Verfahren zum Verhindern des Zugangs, während sich eine Maschine in einem gefährlichen Zustand befindet. Die beiden Bedienungselemente müssen gleichzeitig betätigt werden (mit einem Abstand von 0,5 s), um die Maschine zu starten. Dies stellt sicher, dass beide Hände des Bedieners an einer sicheren Stelle (d. h. an den Schaltern) sein müssen und sich deshalb nicht im Gefahrenbereich befinden können. Die Bedienungselemente müssen kontinuierlich betätigt werden, solange die gefährliche Bedingung vorliegt. Der Maschinenbetrieb muss stoppen, sobald eines der Bedienungselemente losgelassen wird. Wurde ein Bedienungselement losgelassen, kann die Maschine erst wieder gestartet werden, wenn auch das andere Bedienungselement losgelassen wurde.

Ein Steuerungssystem mit 2-Hand-Bedienung stellt hohe Ansprüche an die Integrität des Steuerungs- und Überwachungssystems, damit jeder Fehler erkannt wird. Es ist deshalb wichtig, dass dieser Gesichtspunkt bei der Konstruktion korrekt berücksichtigt wird. Die Leistung der 2-Hand-Sicherheitssysteme wird gemäß ISO 13851 (EN 574) in verschiedene Typen unterteilt (siehe Abbildung), die in etwa den Kategorien der Norm ISO 13849-1 entsprechen. Die Typen, die am häufigsten für die Maschinensicherheit eingesetzt werden, sind IIIB und IIIC. Die folgende Tabelle veranschaulicht den Zusammenhang der Typen mit den Kategorien der Sicherheitsleistung.

Anforderungen	Typen				
	I	II	III		
			A	B	C
Synchrone Auslösung			X	X	X
Verwenden von Kategorie 1 (aus ISO 13849-1)	X		X		
Verwenden von Kategorie 3 (aus ISO 13849-1)		X		X	
Verwenden von Kategorie 4 (aus ISO 13849-1)					X

Der Abstand im physischen Aufbau muss eine unsachgemäße Betätigung (z. B. durch Hand und Ellenbogen) ausschließen. Dies kann durch den Abstand oder durch Abschirmungen erzielt werden. Die Maschine darf nicht von einem Zyklus zum nächsten übergehen, ohne dass beide Taster losgelassen und gedrückt wurden. So wird verhindert, dass beide Taster blockiert werden und die Maschine kontinuierlich arbeitet. Beim Loslassen eines Tasters muss die Maschine stehen bleiben.

Der Einsatz von 2-Hand-Bedienungen ist mit Vorsicht zu betrachten, da normalerweise ein Restrisiko nicht ausgeschlossen werden kann. Die 2-Hand-Bedienung schützt ausschließlich die Person, die diese verwendet. Der geschützte Bediener muss in der Lage sein, den gesamten Zugang zur Gefahrenquelle zu überwachen, da das übrige Personal eventuell nicht geschützt ist.

ISO 13851 (EN 574) bietet zusätzliche Informationen zur 2-Hand-Bedienung.

Zustimmungsschalter

Zustimmungsschalter sind Bedienungselemente, die einem Bediener das Eintreten in einen Gefahrenbereich, während die Gefahr akut ist, nur ermöglichen, wenn er den Zustimmungsschalter in der betätigten Position hält. Sie verwenden Schalter mit zwei oder drei Positionen. Schalter mit zwei Positionen sind deaktiviert, wenn der Aktor nicht betätigt wird. Sie sind aktiviert, wenn der Aktor betätigt wird. Schalter mit drei Positionen sind AUS, wenn deaktiviert (Position 1), EIN wenn sie in der mittleren Position (Position 2) gehalten werden. Sie sind deaktiviert, wenn der Aktor über die mittlere Position (Position 3) hinaus betätigt wird. Bei der

Rückkehr von Position 3 nach 1 darf die Ausgangsschaltung beim Passieren von Position 2 nicht schließen.

Zustimmungsschalter müssen in Verbindung mit anderen Sicherheitsfunktionen eingesetzt werden. Ein typisches Beispiel hierfür ist die kontrollierte Verlangsamung einer Bewegung. Sobald der langsame Modus erreicht ist, kann ein Bediener den Gefahrenbereich betreten, wenn er gleichzeitig den Zustimmungsschalter hält.

Bei Verwendung eines Zustimmungsschalters muss ein Signal darauf hinweisen, dass dieser aktiv ist.

Logikgeräte

Logikgeräte spielen eine zentrale Rolle im sicherheitsbezogenen Teil eines Steuerungssystems. Logikgeräte überprüfen und überwachen das Sicherheitssystem und erlauben entweder das Starten der Maschine oder führen Befehle zum Stoppen der Maschine aus.

Mit verschiedenen Logikgeräten kann eine Sicherheitsarchitektur erstellt werden, die die Anforderungen der Maschine hinsichtlich Komplexität und Funktionalität erfüllt. Kleine festverdrahtete Sicherheitsrelais sind die wirtschaftlichste Lösung für kleinere Maschinen, wenn ein dediziertes Logikgerät zur Vervollständigung der Sicherheitsfunktion erforderlich ist. Modulare und konfigurierbare Sicherheitsrelais werden bevorzugt, wenn zahlreiche unterschiedliche Schutzeinrichtungen und eine minimale Zonensteuerung erforderlich sind. Bei mittleren bis großen und komplexeren Maschinen sind programmierbare Systeme mit dezentralen E/A-Modulen zu bevorzugen.

Sicherheitsrelais

Sicherheitsrelais (auch MSR-Module (Monitoring Safety Relay) genannt) spielen in vielen Sicherheitssystemen eine zentrale Rolle. Diese Module bestehen in der Regel aus mindestens zwei positiv angesteuerten Relais mit zusätzlicher Schaltung, die die Leistung der Sicherheitsfunktion gewährleistet.

Positiv angesteuerte Relais sind spezialisierte „Eiswürfel“-Relais. Sie müssen die Leistungsanforderungen der Norm EN 50025 erfüllen. Grundsätzlich wurden sie konzipiert, um das gleichzeitige Schließen der Öffner- und Schließerkontakte zu verhindern. Neue Entwicklungen ersetzen die elektromechanischen Ausgänge durch sichere Halbleiterausgänge.

Sicherheitsrelais führen zahlreiche Überprüfungen des Sicherheitssystems durch. Beim Einschalten initiieren sie die Einschalt-Selbsttests der internen Komponenten. Wenn die Eingangsgeräte aktiviert werden, vergleicht das MSR-Modul die Ergebnisse der redundanten Eingänge. Sofern zulässig, überprüft das MSR-Modul die externen Aktoren. Sind diese in Ordnung, wartet das MSR-Modul auf ein Rückstellsignal, um seine Ausgänge wieder zu aktivieren.

Die Auswahl des richtigen Sicherheitsrelais hängt von verschiedenen Faktoren ab: Typ des überwachten Geräts, Typ des Rückstellvorgangs, Anzahl und Typ der Ausgänge.

Eingangstypen

Schutzeinrichtungen können mittels unterschiedlicher Methoden anzeigen, dass etwas geschehen ist:

Kontaktverriegelungen und Not-Halt-Geräte: mechanische Kontakte, einkanalig mit einem Öffnerkontakt oder zweikanalig mit zwei Öffnerkontakten. Das MSR-Modul muss in der Lage sein, einen Kanal oder zwei Kanäle zu akzeptieren und eine Querschlusserkennung der zweikanaligen Anordnung bereitstellen.

Berührungslose Sicherheitsschalter und Not-Halt-Geräte: mechanische Kontakte, zweikanalig, ein Schließer- und ein Öffnerkontakt. Das MSR-Modul muss in der Lage sein, verschiedenartige Eingänge zu verarbeiten.

Elektronische Ausgangs-Schaltgeräte: Lichtgitter, Laserscanner und elektronische berührungslose Geräte verfügen über zwei stromliefernde Ausgänge und führen ihre eigene Querschlusserkennung aus. Das MSR-Modul muss in der Lage sein, Querschlusserkennung zu ignorieren.

Schaltmatten: Schaltmatten verursachen einen Kurzschluss zwischen zwei Kanälen. Das MSR-Modul muss in der Lage sein, wiederholten Kurzschlüssen standzuhalten.

Schaltleisten: Einige Schaltleisten sind wie 4-adrige Matten aufgebaut. Einige sind zweiadrig und führen eine Änderung des Widerstands herbei. Das MSR-Modul muss in der Lage sein, einen Kurzschluss oder den geänderten Widerstand zu erkennen.

Spannung: Misst die Gegen-EMK eines Motors während des Auslaufens. Das MSR-Modul muss in der Lage sein, hohe Spannungen zu tolerieren und niedrige Spannungen zu erkennen, während der Motor ausläuft.

Stillstandgeräte: Das MSR-Modul muss in der Lage sein, Pulsketten von verschiedenen, redundanten Sensoren zu erkennen.

2-Hand-Bedienung: Das MSR-Modul muss in der Lage sein, verschiedenartige Schließer- und Öffnereingänge zu erkennen und eine 0,5-s-Zeitmessung sowie Ablaufsteuerungslogik zur Verfügung zu stellen.

Sicherheitsrelais müssen so konzipiert sein, dass eine Schnittstelle zu all diesen Gerätetypen besteht, da diese über verschiedene elektrische Eigenschaften verfügen. Einige MSR-Module können an verschiedene Eingangstypen angeschlossen werden, doch sobald das Gerät ausgewählt wurde, kann das MSR-Modul nur noch eine Schnittstelle zu diesem Gerät zur Verfügung stellen. Der Entwickler muss ein MSR-Modul auswählen, das mit dem Eingangsgerät kompatibel ist.

Eingangsimpedanz

Die Eingangsimpedanz der Sicherheitsrelais bestimmt, wie viele Eingangsgeräte an das Relais angeschlossen und in welchem Abstand die Eingangsgeräte installiert werden können. Beispielsweise hat ein Sicherheitsrelais eine maximal zulässige Eingangsimpedanz von 500 Ohm (~). Ist die Eingangsimpedanz größer als 500~, schaltet es seine Ausgänge nicht. Es ist darauf zu achten, dass die Eingangsimpedanz unter dem angegebenen Höchstwert bleibt. Die Eingangsimpedanz wird durch Länge, Querschnitt und Material der verwendeten Verdrahtung beeinflusst.

Anzahl der Eingangsgeräte

Anhand der Risikobeurteilung lässt sich bestimmen, wie viele Eingangsgeräte an ein Sicherheitsrelais (MSR) anzuschließen sind und wie oft die Eingangsgeräte geprüft werden müssen. Um sicherzustellen, dass Not-Halt-Schaltungen und Schutztürverriegelungen betriebsbereit sind, müssen sie in regelmäßigen Intervallen auf ihre Funktion geprüft werden, wie anhand der Risikobeurteilung festgelegt. Beispiel: Ein Sicherheitsrelais (MSR) mit zweikanaligem Eingang, das an einer verriegelten Schutztür angeschlossen ist, die bei jedem Maschinenzyklus (z. B. mehrmals täglich) geöffnet werden muss, braucht möglicherweise nicht geprüft zu werden. Dies liegt daran, dass jedes Öffnen der Schutztür einen Selbsttest des Sicherheitsrelais sowie der Ein- und Ausgänge des Relais (je nach Konfiguration) bewirkt, um einzelne Fehler zu erkennen. Je häufiger die Schutzvorrichtung geöffnet wird, desto höher muss die Integrität des Prüfprozesses sein.

Ein weiteres Beispiel sind Not-Halt-Schaltungen. Da Not-Halt-Schaltungen üblicherweise nur für Notfälle vorgesehen sind, werden sie selten aktiviert. Deshalb sollte ein Plan für das probeweise Betätigen der Not-Halt-Schaltgeräte erstellt werden, um deren Wirksamkeit nachzuweisen. Wird das Sicherheitssystem auf diese Weise eingesetzt, spricht man auch von einer Beständigkeitsprüfung, und die Zeit zwischen den Beständigkeitsprüfungen wird Prüfintervall genannt. Ein drittes Beispiel sind Zugangstüren zur Justierung von Maschinen, bei denen Not-Halt-Schalter nur selten sinnvoll sind. Auch hier muss ein Programm zur Ausführung einer Funktionsprüfung in regelmäßigen Abständen ausgearbeitet werden.

Mithilfe der Risikobeurteilung lässt sich festlegen, ob die Eingangsgeräte geprüft werden müssen und wie oft Prüfungen erforderlich sind. Je höher das Risiko, desto höher die erforderliche Integrität des Prüfprozesses. Je seltener die automatische Prüfung stattfindet, desto häufiger sollte die manuelle Prüfung vorgenommen werden.

Querschlusserkennung am Eingang

In zweikanaligen Systemen müssen Kurzschlüsse der Eingangsgeräte zwischen Kanälen, auch Querschlussfehler genannt, vom Sicherheitssystem erkannt werden. Diese Erkennung erfolgt über das Sensorgerät oder das Überwachungs-Sicherheitsrelais.

Auf Mikroprozessoren basierende Sicherheitsrelais wie Lichtgitter, Laserscanner und erweiterte, berührungslose Sensoren erkennen diese Querschlüsse auf unterschiedliche Weise. Eine gängige Möglichkeit zum Erkennen von Querschlüssen ist die Verwendung verschiedenartiger Impulstests. Die Ausgangssignale werden in sehr schnellen Impulsen ausgegeben. Der Impuls von Kanal 1 erfolgt zeitlich versetzt vom Impuls von Kanal 2. Tritt ein Kurzschluss auf, erfolgen die Impulse gleichzeitig und werden vom Gerät erkannt.

Elektromechanische Sicherheitsrelais setzen eine andere Technik ein: ein Pull-up-Eingang und ein Pull-down-Eingang. Ein Kurzschluss von Kanal 1 zu Kanal 2 aktiviert das Überstromschutzgerät, woraufhin das Sicherheitssystem abgeschaltet wird.

Ausgänge

MSR-Module werden mit einer unterschiedlichen Anzahl von Ausgängen geliefert. Mithilfe der Ausgangstypen lässt sich bestimmen, welches MSR-Modul in bestimmten Anwendungen verwendet werden muss.

Die meisten MSR-Module verfügen über mindestens zwei gleichzeitig aktive Sicherheitsausgänge. MSR-Sicherheitsausgänge werden als Schließerausgänge charakterisiert. Hierbei handelt es sich um Sicherheitsgeräte, da sie Redundanz und eine interne Prüfung bieten. Ein zweiter Ausgangstyp sind verzögerte Ausgänge. Verzögerte Ausgänge werden in der Regel in Stopps der Kategorie 1 verwendet, bei denen die Maschine die Stoppfunktion ausführen muss, bevor der Zugang zum Gefahrenbereich ermöglicht wird. MSR-Module sind auch mit Hilfsausgängen ausgestattet. Im Allgemeinen sind diese als Öffnerausgänge aufgeführt.

Bemessungsdaten von Ausgängen

Die Bemessungsdaten der Ausgänge beschreiben die Fähigkeit der Schutzeinrichtung, Lasten zu schalten. Üblicherweise werden die Bemessungsdaten industriell genutzter elektrischer Geräte als ohmsche oder elektromagnetische Lasten angegeben. Eine ohmsche Last kann eine LED oder ein Widerstandsheizelement sein. Bei elektromagnetischen Lasten handelt es sich in der Regel um Relais, Schütze oder Magnetspulen. Die Last ist dabei äußerst induktiv. In Anhang A der Norm IEC 60947-5-1 sind die Lastkenndaten beschrieben. Weitere Informationen hierzu enthält auch der Abschnitt zu den Grundsätzen im Sicherheitskatalog.

Kennbuchstabe: Die Bezeichnung ist ein Buchstabe, auf den eine Zahl folgt, z. B. A300. Der Buchstabe bezieht sich auf den konventionellen thermischen Strom von gekapselten Geräten und gibt an, ob es sich um Gleichstrom oder um Wechselstrom handelt. Zum Beispiel steht A für 10 Ampere Wechselstrom. Die Zahl gibt die Bemessungs-Isolationsspannung an. Zum Beispiel steht 300 für 300 Volt.

Gebrauchskategorie: Die Gebrauchskategorie beschreibt die Arten von Lasten, für die das Gerät ausgelegt ist. Die für IEC 60947-5 relevanten Gebrauchskategorien sind in der folgenden Tabelle aufgeführt.

Gebrauchskategorie	Beschreibung der Last
AC-12	Schalten ohmscher und elektronischer Lasten mit Trennung durch Optokoppler
AC-13	Schalten von Halbleiterlast mit Trennung durch Transformator
AC-14	Steuerung kleiner elektromagnetischer Lasten (unter 72 VA)
AC-15	Elektromagnetische Lasten über 72 VA
DC-12	Schalten ohmscher und elektronischer Lasten mit Trennung durch Optokoppler
DC-13	Schalten von Elektromagneten bei Gleichspannung
DC-14	Schalten induktiver Lasten mit Sparwiderständen im Stromkreis

Thermischer Strom Ith: Der konventionelle thermische Strom von gekapselten Geräten ist der Wert des Stroms, der für Erwärmungsprüfungen der Geräte beim Einbau in ein bestimmtes Gehäuse verwendet wird.

Bemessungs-Betriebsspannung (Ue) und Bemessungs-Betriebsstrom (Ie): Diese geben das Ein- und Ausschaltvermögen der Schaltelemente unter normalen Betriebsbedingungen an. Die Produkte der Serie Allen-Bradley Guardmaster sind für 125 V AC, 250 V AC und 24 V DC ausgelegt. Falls andere als die angegebenen Spannungen verwendet werden sollen, ist das Werk zu konsultieren.

VA: Der VA-Wert (Volt x Ampere) gibt die Bemessungswerte der Schaltelemente beim Schließen und Öffnen des Stromkreises an.

Beispiel 1: Ein Wert von A150/AC-15 bedeutet, dass die Kontakte einen 7200-VA-Stromkreis schließen können. Bei 120 V AC können die Kontakte einen Einschaltstrom von 60 Ampère bewältigen. Da AC-15 eine elektromagnetische Last ist, liegen die 60 Ampere nur kurzzeitig an (Einschaltstromstoß der elektromagnetischen Last). Beim Öffnen des Stromkreises sind nur 720 VA zulässig, denn der Dauerstrom der elektromagnetischen Last beträgt 6 A, was dem Bemessungs-Betriebsstrom entspricht.

Beispiel 2: Ein Wert von N150/DC-13 bedeutet, dass die Kontakte einen 275-VA-Stromkreis schließen können. Bei 125 V AC können die Kontakte einen Einschaltstrom von 2,2 Ampère bewältigen. Elektromagnetische Gleichstromlasten haben keinen Einschaltstrom wie elektromagnetische Wechselstromlasten. Auch beim Öffnen des Stromkreises sind 275 VA zulässig, denn der Dauerstrom der elektromagnetischen Last beträgt 2,2 A, was dem Bemessungs-Betriebsstrom entspricht.

Wiederanlauf von Maschinen

Wenn beispielsweise eine verriegelte Schutztür an einer laufenden Maschine geöffnet wird, stoppt der Sicherheits-Verriegelungsschalter die Maschine. In den meisten Fällen ist es eine zwingende Notwendigkeit, dass die Maschine nicht sofort nach dem Schließen der Schutztür wieder anläuft. Dies wird üblicherweise über einen Anlauf mit selbsthaltendem Schütz erreicht.

Durch kurzes Drücken des Starttasters wird die Steuerspule im Schütz aktiviert, wodurch die Schaltkontakte schließen. Solange Strom über die Schaltkontakte fließt, bleibt die Steuerspule durch die mechanisch mit den Schaltkontakten verbundenen Hilfskontakte des Schützes erregt (elektrisch gerastet). Bei Unterbrechung der Hauptspannung oder Steuerspannung wird die Spule stromlos, während die Arbeitsstrom- und Hilfskontakte öffnen. Die Verriegelung der Schutztür ist im Steuerstromkreis des Schützes verdrahtet. Dies bedeutet, dass Wiederanlauf nur möglich ist, wenn die Schutztür geschlossen und die Maschine anschließend mit dem normalen Einschaltknopf in Betrieb gesetzt wird. Dadurch wird das Schütz zurückgestellt, woraufhin die Maschine wieder anläuft.

Die Anforderung für normale Verriegelungssituationen regelt ISO 12100-1, Absatz 3.22.4 (Auszug):

Bei geschlossener Schutzvorrichtung sind die von der Schutzvorrichtung abgedeckten gefährlichen Maschinenfunktionen betriebsfähig, doch das Schließen der Schutzvorrichtung selbst darf nicht die Maschine in Betrieb setzen.

Viele Maschinen besitzen bereits Einfach- oder Doppelschütze, die wie oben beschrieben funktionieren (oder sie sind mit einem System ausgestattet, mit dem das gleiche Ergebnis erreicht wird). Beim Nachrüsten einer Verriegelung an vorhandenen Maschinen ist zu prüfen, ob die Steueranordnung für den Arbeitsstrom dieser Anforderung entspricht. Gegebenenfalls sind zusätzliche Maßnahmen zu ergreifen.

Rückstellfunktionen

Allen Bradley Guardmaster-Sicherheitsrelais sind für überwachte manuelle Rückstellung oder automatische/manuelle Rückstellung ausgelegt.

Überwachte manuelle Rückstellung

Eine überwachte manuelle Rückstellung erfordert eine Zustandsänderung des Rückstellkreises, nachdem die Tür geschlossen oder das Not-Halt-Schaltgerät zurückgesetzt wurde. Die mechanisch verbundenen Hilfs-Öffnungskontakte der Leistungsschaltschütze sind mit einem Taster in Reihe geschaltet. Nachdem die Schutztür geöffnet und wieder geschlossen wurde, lässt das Sicherheitsrelais erst dann einen Wiederanlauf der Maschine zu, wenn am Rückstelltaster eine Zustandsänderung aufgetreten ist. Dies ist konform mit den Anforderungen hinsichtlich einer zusätzlichen Rückstellung von Hand gemäß EN ISO 13849-1, d. h. die Rückstellfunktion gewährleistet, dass sich beide Schütze im AUS-Zustand befinden und beide Verriegelungskreise (und damit die Schutztüren) geschlossen sind. Da außerdem eine Zustandsänderung erforderlich ist, wird so sichergestellt, dass der Rückstellbetätiger nicht umgangen oder auf irgendeine Weise blockiert wurde. Werden diese Prüfungen erfolgreich bestanden, kann die Maschine über die normalen Bedienungselemente neu gestartet werden. EN ISO 13849-1 führt die Zustandsänderung vom eingeschalteten zum ausgeschalteten Zustand an, doch dasselbe Schutzprinzip kann auch durch den gegenteiligen Effekt erzielt werden.

Der Rückstellschalter muss sich an einer Stelle mit guter Sicht auf den Gefahrenbereich befinden, damit der Bediener vor dem Einschalten der Maschine den Bereich überprüfen kann.

Automatische/manuelle Rückstellung

Einige Sicherheitsrelais ermöglichen eine automatische/manuelle Rückstellung. Der Modus für die manuelle Rückstellung wird nicht überwacht, d. h. die Rückstellung erfolgt, sobald die Taste gedrückt wird. Ein Kurzschluss oder eine Blockierung des Rückstellschalters wird nicht erkannt. Bei diesem Ansatz können eventuell die Anforderungen einer zusätzlichen Rückstellung von Hand, wie in EN ISO 13849-1 angegeben, nur mithilfe zusätzlicher Mittel erfüllt werden.

Alternativ hierzu kann die Rückstellleitung überbrückt werden, was eine automatische Rückstellung ermöglicht. Der Maschinenbetreiber muss dann einen anderen Mechanismus vorsehen, um ein Anlaufen der Maschine beim Schließen der Schutztür zu verhindern.

Ein Gerät zur automatischen Rückstellung erfordert keinen manuellen Schalteingriff, doch nach einer Schutzabschaltung wird das System stets auf Integrität geprüft, bevor die Rückstellung erfolgt. Ein System mit automatischer Rückstellung darf nicht mit einem Gerät ohne Rückstellung verwechselt werden. Bei letzterem wird das Sicherheitssystem sofort nach einer Schutzabschaltung wieder aktiviert, ohne die Integrität des Systems zu prüfen.

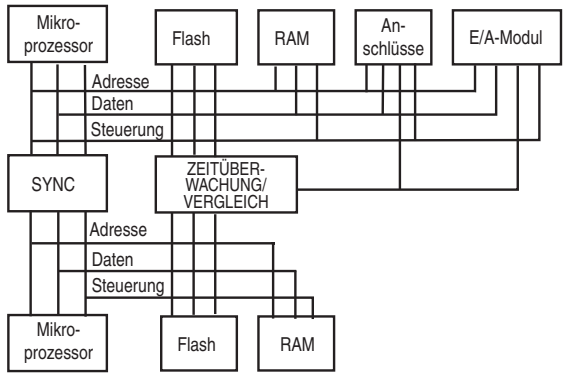
Der Rückstellschalter muss sich an einer Stelle mit guter Sicht auf den Gefahrenbereich befinden, damit der Bediener vor dem Einschalten der Maschine den Bereich überprüfen kann.

Schutzvorrichtungen ohne Wiederanlaufsperre

Eine Schutzvorrichtung ohne Wiederanlaufsperre stoppt eine Maschine, wenn die Schutzvorrichtung geöffnet wird. Beim Schließen der Schutzvorrichtung läuft die Maschine sofort wieder an. Schutzvorrichtungen ohne Wiederanlaufsperre sind nur unter bestimmten eingeschränkten Bedingungen zulässig, da ein unerwarteter Anlauf oder ein unerwarteter Ausfall des Ausschaltsystems äußerst gefährlich wäre. Das Verriegelungssystem muss die höchstmögliche Zuverlässigkeit aufweisen (oft ist es ratsam, eine Schutzverriegelung vorzusehen). Die Verwendung von Schutzvorrichtungen ohne Wiederanlaufsperre kommt NUR an Maschinen in Frage, bei denen NICHT die Möglichkeit besteht, dass ein Bediener oder ein Teil seines Körpers bei geschlossener Schutzvorrichtung in der Gefahrenzone bleibt oder in die Gefahrenzone hineinreicht. Die Schutzvorrichtung ohne Wiederanlaufsperre muss der einzige Zugang zum Gefahrenbereich sein.

Sicherheitsprogrammierbare Logiksteuerungen

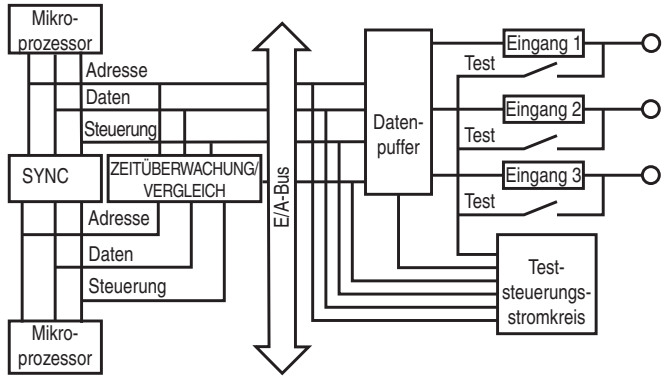
Der Bedarf an flexiblen und skalierbaren Sicherheitsanwendungen führte zur Entwicklung von Sicherheits-SPS bzw. Sicherheitssteuerungen. Programmierbare Sicherheitssteuerungen bieten den Anwendern dieselbe Steuerungsflexibilität in einer Sicherheitsanwendung, die sie von programmierbaren Standardsteuerungen gewohnt sind. Allerdings gibt es erhebliche Unterschiede zwischen Standard- und Sicherheits-SPS. Sicherheits-SPS werden in verschiedenen Plattformen ausgeliefert, um der Skalierbarkeit sowie den Funktions- und Integrationsanforderungen der komplexeren Sicherheitssysteme gerecht zu werden.



1oo2D-Architektur

Es werden mehrere Mikroprozessoren zur Verarbeitung von E/A, Speicher und Sicherheitskommunikation verwendet. Überwachungsschaltkreise führen Diagnoseanalysen aus. Dieser Aufbau wird auch als 1oo2D bezeichnet, da einer der beiden Mikroprozessoren die Sicherheitsfunktion ausführen kann und umfangreiche Diagnosefunktionen ausgeführt werden, um sicherzustellen, dass beide Mikroprozessoren synchron arbeiten.

Darüber hinaus wird jede Eingangsschaltung in jeder Sekunde zahlreichen internen Tests unterzogen, wodurch ihre ordnungsgemäße Funktion sichergestellt wird. Vielleicht betätigen Sie den Not-Halt-Schalter nur einmal im Monat. Doch wenn Sie ihn betätigen, wurde sein Schaltkreis bis zu diesem Zeitpunkt kontinuierlich getestet, sodass das Not-Halt-Signal in der Sicherheits-SPS richtig erkannt wird.



Blockdiagramm mit Sicherheitseingangsmodul

Ausgänge von Sicherheits-SPS sind elektromechanische Ausgänge oder elektronische Sicherheitsausgänge. Genau wie die Eingangsschaltungen werden auch die Ausgangsschaltungen mehrmals pro Sekunde getestet, um sicherzustellen, dass sie den Ausgang deaktivieren können. Wenn bei einem der drei Ausgänge ein Fehler auftritt, wird dieser von den beiden anderen Ausgängen deaktiviert und der Fehler wird vom internen Überwachungsschaltkreis gemeldet.

Bei Verwendung von Sicherheitsgeräten mit mechanischen Kontakten (Not-Halt-Schalter, Gate-Schalter usw.) kann der Anwender Impulstestsignale anwenden, um Querschlüsse zu erkennen. Damit die teuren Sicherheitsausgänge nicht überbelastet werden, stellen viele Sicherheits-SPS spezielle Impulsausgänge zur Verfügung, die an mechanische Kontaktgeräte angeschlossen werden können.

Software

Sicherheits-SPS lassen sich im Großen und Ganzen wie Standard-SPS programmieren. Alle zuvor erwähnten zusätzlichen Diagnosefunktionen und Fehlerprüfungen werden vom Betriebssystem ausgeführt, sodass dem Programmierer noch nicht einmal bewusst ist, dass diese stattfinden. Die meisten Sicherheits-SPS verfügen über spezielle Befehle zum Schreiben des Programms für das Sicherheitssystem. Diese Befehle imitieren die Funktionen ihrer Sicherheitsrelais-Gegenstücke. Beispielsweise funktioniert der Not-Halt-Befehl ähnlich wie ein MSR 127. Doch auch wenn die Logik, auf der diese Befehle basieren, äußerst komplex ist, sehen die Sicherheitsprogramme relativ einfach aus, da der Programmierer diese Blöcke einfach miteinander verbinden muss. Diese Befehle werden zusammen mit anderen logischen, mathematischen oder datenbezogenen Manipulationen (z. B. Befehle) durch Dritte zertifiziert. Auf diese Weise wird sichergestellt, dass ihre Funktion mit den gültigen Industrienormen konsistent ist.

Funktionsblöcke sind das vorherrschende Verfahren für das Programmieren von Sicherheitsfunktionen. Neben Funktionsblöcken und Kontaktplanlogik bieten Sicherheits-SPS auch zertifizierte Befehle für Sicherheitsanwendungen. Zertifizierte Sicherheitsbefehle ermöglichen ein anwendungsspezifisches Verhalten. Dieses Beispiel zeigt einen Not-Halt-Befehl. Um dieselbe Funktion in Kontaktplanlogik zu erstellen, wären etwa 16 Strompfade mit Kontaktplanlogik erforderlich. Da das Logikverhalten bereits im Not-Halt-Befehl integriert ist, muss die integrierte Logik nicht getestet werden.

Zertifizierte Funktionsblöcke stehen zur Verfügung, um eine Schnittstelle zu fast allen Sicherheitsgeräten zu ermöglichen. Eine Ausnahme ist die Sicherheitsleiste mit Widerstandstechnologie.

Sicherheits-SPS generieren eine „Signatur“, dank der verfolgt werden kann, ob Änderungen vorgenommen wurden. Diese Signatur besteht in der Regel aus einer Kombination des Programms, der Eingangs-/Ausgangskonfiguration und einer Zeitmarke. Wenn das Programm abgeschlossen und validiert wurde, muss der Anwender diese Signatur als Teil der Validierungsergebnisse notieren, um später darauf zurückgreifen zu können. Falls das Programm geändert werden muss, ist eine erneute Validierung erforderlich und es muss eine neue Signatur notiert werden. Das Programm kann auch durch ein Kennwort gesperrt werden, um unbefugte Änderungen zu verhindern.

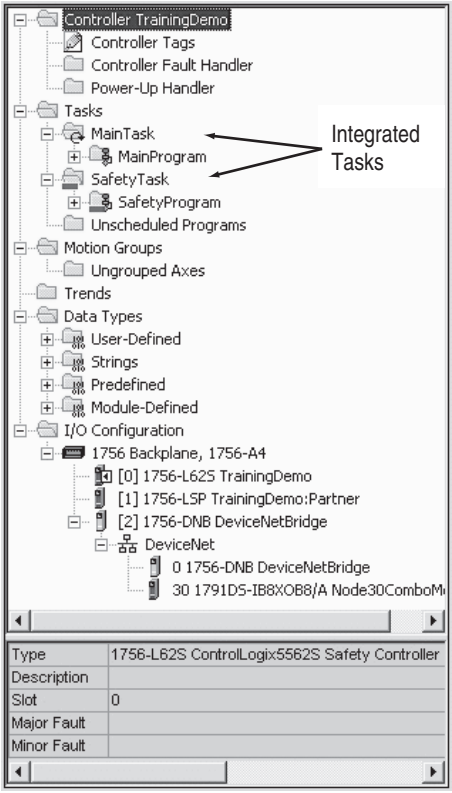
Die Verdrahtung ist im Vergleich zu Sicherheitsrelais dank der programmierbaren Logiksysteme wesentlich einfacher. Anstatt bestimmte Klemmen an den Sicherheitsrelais zu verdrahten, werden die Eingangsgeräte an beliebige Eingangsklemmen angeschlossen, während Ausgangsgeräte an beliebige Ausgangsklemmen angeschlossen werden. Anschließend ordnet die Software die Klemmen zu.

Integrierte Sicherheitssteuerungen

Sicherheitssteuerungslösungen können jetzt vollständig in eine einzige Steuerungsarchitektur integriert werden, die miteinander kooperierende Sicherheits- und Standardsteuerungsfunktionen umfasst. Die Möglichkeit, Achssteuerungs-, Antriebs-, Prozess-, Batch-, sequenzielle Hochgeschwindigkeits- und SIL3-Sicherheit in einer Steuerung vereinen zu können, sorgt für signifikante Vorteile. Die Integration von Sicherheits- und Standardsteuerung ermöglicht die Nutzung gemeinsamer Tools und Technologien, was die Kosten für Entwicklung, Installation, Inbetriebnahme und Instandhaltung erheblich senkt. Da eine gemeinsame Steuerungshardware, dezentrale Sicherheits-E/A oder Geräte in Sicherheitsnetzwerken bzw. gemeinsame Bedienerschnittstellengeräte verwendet werden können, sind auch die Anschaffungs- und Instandhaltungskosten geringer und die Entwicklungszeiten kürzer. Alle diese Merkmale sorgen für mehr Produktivität, eine schnellere Fehlerbehebung und niedrigere Schulungskosten.

Die folgende Abbildung zeigt ein Beispiel für die Integration von Steuerung und Sicherheit. Die nicht sicherheitsbezogenen Standardsteuerungsfunktionen befinden sich unter der Hauptaufgabe (MainTask). Die sicherheitsbezogenen Funktionen befinden sich unter der Sicherheitsaufgabe (SafetyTask).

Alle Standard- und Sicherheitsfunktionen sind voneinander isoliert. Beispielsweise können Sicherheits-Tags direkt von der Standardlogik gelesen werden. Die Sicherheits-Tags lassen sich zwischen GuardLogix-Steuerungen über EtherNet, ControlNet oder DeviceNet austauschen. Die Daten der Sicherheits-Tags können direkt von externen Geräten, Bedienerschnittstellen, PCs oder anderen Steuerungen gelesen werden.



1. Standard-Tags und Logik weisen dasselbe Verhalten auf wie ControlLogix.

2. Standard-Tag-Daten, programm- oder steuerungsbezogene Daten können von externen Geräten, Bedienerschnittstellen, PCs und anderen Steuerungen usw. gelesen werden.

3. Als integrierte Steuerung ermöglicht GuardLogix das Verschieben (Zuordnen) von Standard-Tag-Daten in Sicherheits-Tags, um diese innerhalb der Sicherheitsaufgabe verwenden zu können. Dies hat den Vorteil, dass Anwender die Statusinformationen von der Standardseite der GuardLogix-Steuerung lesen können. Diese Daten dürfen nicht für die direkte Steuerung eines Sicherheitsausgangs verwendet werden.

4. Sicherheits-Tags können direkt von der Standardlogik gelesen werden.

5. Sicherheits-Tags können von der Sicherheitslogik gelesen oder geschrieben werden.

6. Die Sicherheits-Tags lassen sich zwischen GuardLogix-Steuerungen über EtherNet austauschen.

7. Sicherheits-Tag-Daten, programm- oder steuerungsbezogene Daten können von externen Geräten, Bedienerschnittstellen, PCs, anderen Steuerungen usw. gelesen werden. Beachten Sie, dass diese Daten nach dem Lesevorgang als Standarddaten und nicht als Sicherheitsdaten betrachtet werden.

Sicherheitsnetzwerke

Bisher haben Kommunikationsnetzwerke im Fertigungsbereich dafür gesorgt, dass Hersteller die Flexibilität verbessern, Diagnosefunktionen erweitern, Abstände vergrößern, Installations- und Verdrahtungskosten senken, die Wartungsfreundlichkeit erhöhen und die Produktivität ihrer Fertigungsprozesse im Allgemeinen verbessern konnten. Dieselbe Motivation hat auch die Realisierung industrieller Sicherheitsnetzwerke vorangetrieben. Diese Sicherheitsnetzwerke ermöglichen es den Herstellern, Sicherheits-E/A und Sicherheitsgeräte in ihren Maschinen mithilfe eines einzigen Netzwerkkabels zu verteilen. Auf diese Weise werden die Installationskosten gesenkt, während die Diagnosefunktionen verbessert werden. Gleichzeitig ist eine komplexere Gestaltung der Sicherheitssysteme möglich. Außerdem sorgen Sicherheitsnetzwerke für eine sichere Kommunikation zwischen Sicherheits-SPS bzw. Sicherheitssteuerungen, damit die Anwender ihre Sicherheitssteuerung auf verschiedene intelligente Systeme verteilen können.

Sicherheitsnetzwerke verhindern nicht das Auftreten von Kommunikationsfehlern. Sie können vielmehr Übertragungsfehler erkennen und anschließend Sicherheitsgeräten erlauben, die entsprechenden Maßnahmen zu ergreifen. Es können beispielsweise folgende Kommunikationsfehler erkannt werden: Einfügen von Nachrichten, verloren gegangene Nachrichten, fehlerhafte Nachrichten, verzögerte Nachrichten, wiederholt gesendete Nachrichten und eine falsche Reihenfolge der Nachrichten.

Wenn bei den meisten Anwendungen ein Fehler erkannt wird, wechselt das Gerät in einen bekannten Ruhezustand, der in der Regel „sicherer Zustand“ genannt wird. Der Sicherheitseingang oder das Ausgangsgerät ist für das Erkennen dieser Kommunikationsfehler verantwortlich. Anschließend muss ggf. in den sicheren Zustand gewechselt werden.

Die frühen Sicherheitsnetzwerke waren an einen bestimmten Medientyp oder ein Medienzugriffsschema gebunden, sodass die Hersteller bestimmte Kabel, Netzwerkschnittstellenkarten, Router, Bridges usw. verwenden mussten, die dann auch Teil der Sicherheitsfunktion wurden. Diese Netzwerke konnten nur die Kommunikation zwischen Sicherheitsgeräten unterstützen. Dies hatte zur Folge, dass Hersteller zwei oder mehr Netzwerke für die Steuerungsstrategie ihrer Maschinen einsetzen mussten (ein Netzwerk für die Standardsteuerung und ein weiteres für die Sicherheitssteuerung) – und natürlich waren auch die Kosten für Installation, Schulung und Ersatzteile wesentlich höher.

Bei modernen Sicherheitsnetzwerken kann über ein einziges Kabel mit Sicherheits- und Standardsteuergeräten kommuniziert werden. Das CIP-Sicherheitsprotokoll (Common Industrial Protocol; modernes Industrieprotokoll) ist ein offenes Standardprotokoll, das von der ODVA (Open DeviceNet Vendors Association) veröffentlicht wurde. Es ermöglicht die sichere Kommunikation zwischen Sicherheitsgeräten in DeviceNet-, ControlNet- und EtherNet/IP-Netzwerken. Da das CIP-Sicherheitsprotokoll eine Erweiterung des CIP-Standardprotokolls ist, können Sicherheitsgeräte und Standardgeräte gemeinsam im selben Netzwerk eingesetzt werden. Die Anwender können auch Bridges zwischen Netzwerken mit Sicherheitsgeräten aufbauen. Auf diese Weise lassen sich Sicherheitsgeräte zur Feinabstimmung der Sicherheitsreaktionszeiten

aufteilen oder einfacher verteilen. Da das Sicherheitsprotokoll in der alleinigen Verantwortung der Endgeräte liegt (Sicherheits-SPS bzw. Sicherheitssteuerung, Sicherheits-E/A-Modul, Sicherheitskomponente), werden standardmäßige Kabel, Netzwerkschnittstellenkarten, Bridges und Router verwendet und machen spezielle Netzwerkhardware oder das Entfernen dieser Geräte aus der Sicherheitsfunktion überflüssig.

Ausgangsgeräte

Sicherheitshilfsschütze und Sicherheitsschütze

Hilfsschütze und Schütze dienen dazu, die Stromzufuhr zum Aktor zu unterbrechen. Die Hilfsschütze und Schütze werden um spezielle Leistungsmerkmale ergänzt, um die Sicherheitsklassifizierung zu erreichen.

Mechanisch verbundene Öffnerkontakte führen den Status der Hilfsschütze und Schütze an das Logikgerät zurück. Durch die Verwendung mechanisch verbundener Kontakte wird die Sicherheitsfunktion gewährleistet. Damit die Anforderungen mechanisch verbundener Kontakte erfüllt werden, dürfen sich die Öffner- und Schließerkontakte nicht gleichzeitig im geschlossenen Zustand befinden. IEC 60947-5-1 definiert die Anforderungen für mechanisch verbundene Kontakte. Falls die Schließerkontakte verschweißen würden, bleiben die Öffnerkontakte um mindestens 0,5 mm geöffnet. Umgekehrt gilt, dass beim Verschweißen der Öffnerkontakte die Schließerkontakte geöffnet blieben.

Sicherheitssysteme dürfen nur in bestimmten Positionen gestartet werden. Standardhilfsschütze und -schütze ermöglichen das Eindrücken des Ankers, um die Schließerkontakte zu schließen. Bei Sicherheitsgeräten ist der Anker vor einer manuellen Überbrückung geschützt, um ein unerwartetes Anlaufen zu verhindern.

Bei Sicherheitshilfsschützen wird der Öffnerkontakt durch den Hauptschlüssel betätigt. Sicherheitsschütze verwenden einen Hilfsschalter, um die mechanisch verbundenen Kontakte zu lokalisieren. Falls der Kontaktblock von der Basis fällt, bleiben die mechanisch verbundenen Kontakte geschlossen. Die mechanisch verbundenen Kontakte sind dauerhaft am Sicherheitshilfsschütz oder Sicherheitsschütz befestigt. Bei größeren Schützen reicht ein Hilfsschalter nicht aus, um den Status des breiteren Schlüssels widerzuspiegeln. Es werden die in Abbildung 4.81 dargestellten Spiegelkontakte verwendet, die sich auf beiden Seiten des Schützes befinden.

Die Ausfallzeit der Hilfsschütze oder Schütze spielen bei der Berechnung des Sicherheitsabstands eine Rolle. Häufig wird ein Überspannungsschutz auf der Spule angebracht, um die Betriebsdauer der Kontakte, die die Spule ansteuern, zu verlängern. Bei AC-Spulen ist die Ausfallzeit nicht betroffen. Bei DC-Spulen wird die Ausfallzeit verlängert. Die Verlängerung hängt vom Typ der ausgewählten Unterdrückung ab.

Hilfsschütze und Schütze sind für die Umschaltung großer Lasten zwischen 0,5 A und über 100 A konzipiert. Das Sicherheitssystem funktioniert bei niedrigen Strömen. Das vom Logikgerät des Sicherheitssystems generierte Rückführungssignal kann einige wenige

Milliampere oder bis zu 10, 20 oder mehr Milliampere aufweisen (in der Regel 24 V DC). Die Sicherheitshilfsschütze und Sicherheitsschütze verwenden vergoldete, geschlitzte Kontakte, um diese kleinen Ströme zuverlässig schalten zu können.

Überlastschutz

Laut Elektronormen ist für Motoren ein Überlastschutz erforderlich. Die vom Überlastschutzgerät zur Verfügung gestellten Diagnosen verbessern nicht nur die Sicherheit der Anlagen, sondern auch die der Bediener. Die heute verfügbaren Technologien erkennen Fehlerbedingungen wie Überlast, Phasenverlust, Erdschluss, Abschaltung, Blockierung, Unterlast, Stromasymmetrie und Übertemperatur. Das Erkennen und Kommunizieren anormaler Bedingungen, bevor diese zu einer Auslösung führen, ermöglicht kürzere Produktionszeiten und verhindert, dass Bediener und Wartungspersonal unvorhergesehenen Gefahren ausgesetzt werden.

Frequenzumrichter und Servoantriebe

Sicherheitsantriebe und -servoantriebe sollen verhindern, dass die Rotationsenergie unterdrückt wird, um einen Sicherheitsstopp und einen Not-Halt zu erzielen.

Frequenzumrichter erzielen die Sicherheitsklassifizierung durch redundante Kanäle, die die Stromzufuhr zur Gate-Steuerungsschaltung des Leistungsteils unterbrechen. Ein Kanal ist die Hardware-Freigabe (HW Enable), welche das Eingangssignal zur Gate-Steuerungsschaltung unterbricht. Der zweite Kanal ist das positiv angesteuerte Relais, das die Speisung der Gate-Steuerungsschaltung unterbricht. Das positiv angesteuerte Relais hat einen zwangsgeführten Kontakt, welcher als Statussignal für das Logiksystem verwendet wird. Durch dieses redundante Konzept kann der Frequenzumrichter in Not-Halt-Schaltkreisen eingesetzt werden, ohne dass ein Schütz erforderlich ist.

Der Servoantrieb erzielt sein Ergebnis auf ähnliche Weise wie Frequenzumrichter durch redundante Sicherheitssignale, mit denen die Sicherheitsfunktion ausgelöst wird. Ein Signal unterbricht die Versorgung der Gate-Steuerungsschaltung. Ein zweites Signal unterbricht die Stromversorgung des Netzteils der Gate-Steuerungsschaltung. Es werden zwei positiv angesteuerte Relais verwendet, um die Signale zu löschen und Feedback an das Sicherheitslogikgerät zurückzusenden.

Verbindungssysteme

Verbindungssysteme sorgen für Mehrwert, da die Installations- und Instandhaltungskosten der Sicherheitssysteme verringert werden. Bei der Entwicklung muss überlegt werden, ob ein Kanal, zwei Kanäle, zwei Kanäle mit Anzeige oder mehrere Gerätetypen verwendet werden.

Wenn eine Reihenschaltung von zweikanaligen Verriegelungen erforderlich ist, kann ein Verteilerkasten die Installation vereinfachen. Mit einer IP67-Klassifizierung können diese Gehäusetypen an Maschinen dezentraler Standorte montiert werden. Wenn ein diversitäres Geräteset erforderlich ist, kann ein ArmorBlock Guard I/O-Gehäuse verwendet werden. Die Eingänge lassen sich über die Software konfigurieren, um verschiedene Gerätetypen berücksichtigen zu können.

Berechnen des Sicherheitsabstands

Gefahrenquellen müssen einen sicheren Zustand aufweisen, bevor sich ein Bediener der Gefahrenquelle nähert. Für die Berechnung des Sicherheitsabstands stehen zwei weit verbreitete Normengruppen zur Verfügung. In diesem Kapitel werden diese Normen wie folgt unterteilt:

ISO/EN: (ISO 13855 und EN 999)

US/CAN (ANSI B11.19, ANSI RIA R15.06 und CAN/CSA Z434-03)

Formel

Der minimale Sicherheitsabstand hängt von der Zeit ab, die zum Verarbeiten des Stoppbefehls erforderlich ist. Außerdem muss berücksichtigt werden, wie weit der Bediener in die Erkennungszone eindringen kann, bevor er erkannt wird. Die weltweit verwendete Formel hat dasselbe Format und dieselben Anforderungen. Unterschiedlich sind die Symbole, die zum Darstellen der Variablen verwendet werden, sowie die Maßeinheiten.

Diese Formeln lauten wie folgt:

ISO/EN: S = K x T + C

US/CAN: Ds = K x (Ts + Tc + Tr + Tbm) + Dpf

Dabei stehen Ds und S für den Mindestsicherheitsabstand von der Gefahrenzone bis zum nächsten Erkennungspunkt

Annäherungsrichtungen

Beim Berechnen des Sicherheitsabstands für eine Anwendung, in der ein Lichtgitter oder Bereichsscanner verwendet wird, muss die Annäherung an das Erkennungsgerät berücksichtigt werden. Es werden drei Annäherungstypen berücksichtigt:

Normal – Eine Annäherung im rechten Winkel zur Erkennungsebene

Horizontal – Eine Annäherung parallel zur Erkennungsebene

Winklig – Eine Annäherung in einem bestimmten Winkel zur Erkennungszone.

Geschwindigkeitskonstante

K ist eine Geschwindigkeitskonstante. Der Wert dieser Geschwindigkeitskonstante hängt von den Bewegungen des Bedieners ab (d. h. Handgeschwindigkeiten, Gehgeschwindigkeiten und Schrittlängen). Dieser Parameter basiert auf Forschungsdaten. In der Regel kann bei einem Bediener von einer Handgeschwindigkeit von 1600 mm/s ausgegangen werden, während sich der Körper nicht bewegt. Die Umstände der tatsächlichen Applikation sind zu berücksichtigen. Als allgemeine Richtlinie kann gelten, dass die Annäherungsgeschwindigkeit zwischen 1600 mm/s und 2500 mm/s liegt. Die richtige Geschwindigkeitskonstante muss durch die Risikobeurteilung bestimmt werden.

Stoppzeit

T ist die Gesamtzeit, die das System bis zum vollständigen Stopp benötigt. Die Gesamtzeit (in Sekunden) beginnt ab der Initiierung des Stoppsignals und endet mit dem Ende der Gefahr. Diese Zeit kann in ihre inkrementalen Bestandteile (Ts, Tc, Tr und Tbm) gegliedert werden, um eine einfachere Analyse zu ermöglichen. Ts ist die Stoppzeit der Maschine bzw. des Geräts im ungünstigsten Fall. Tc ist die Stoppzeit des Steuerungssystems im ungünstigsten Fall. Tr ist die Reaktionszeit der Schutzeinrichtung (einschließlich seiner Schnittstelle). Tbm ist die zusätzliche Stoppzeit, die die Bremsenüberwachung zulässt, bevor eine Verschlechterung der Stoppzeit außerhalb der vom Endanwender vorab festgelegten Grenzwerte erkannt wird. Tbm wird für mechanische Pressen mit Schwungrad eingesetzt. Ts + Tc + Tr werden normalerweise mit einer Stoppuhr bestimmt, wenn die Werte unbekannt sind.

Faktoren für die Eindringtiefe

Die Faktoren für die Eindringtiefe werden durch die Symbole C und Dpf dargestellt. Es handelt sich um den maximalen Weg bis zur Gefahrenquelle, bevor das Eindringen durch die Schutzeinrichtung erkannt wird. Die Faktoren für die Eindringtiefe ändern sich abhängig vom Gerätetyp und der Anwendung. Ziehen Sie die entsprechende Norm zu Rate, um den optimalen Eindringtiefenfaktor zu bestimmen. Für eine normale Annäherung an ein Lichtgitter oder einen Bereichsscanner, dessen Objektempfindlichkeit unter 64 mm liegt, verwenden die ANSI- und kanadischen Normen folgende Formel:

Dpf = 3,4 x (Objektempfindlichkeit – 6,875 mm), doch keinen kleineren Wert als 0.

Für eine normale Annäherung an ein Lichtgitter oder einen Bereichsscanner, dessen Objektempfindlichkeit unter 40 mm liegt, verwenden die ISO- und EN-Normen folgende Formel:

C = 8 x (Objektempfindlichkeit – 14 mm), doch keinen kleineren Wert als 0

Diese beiden Formeln haben einen Überschneidungspunkt bei 19,3 mm. Bei einer Objektempfindlichkeit von unter 19 mm unterliegt die Herangehensweise laut den US- und kanadischen Normen größeren Einschränkungen, da das Lichtgitter bzw. der Bereichsscanner weiter von der Gefahrenquelle entfernt sein muss. Für Objektempfindlichkeiten über 19,3 mm ist die ISO/EN-Norm restriktiver. Maschinenbauer, die eine Maschine für den weltweiten Einsatz konstruieren möchten, müssen aus beiden Gleichungen die Bedingungen im ungünstigsten Fall berücksichtigen.

Durchgriffsanwendungen

Wenn größere Objektempfindlichkeiten verwendet werden, unterscheiden sich die US/CAN- und die ISO/EN-Normen geringfügig hinsichtlich des Faktors für die Eindringtiefe und der Objektempfindlichkeit. Der ISO/EN-Wert lautet 850 mm, während der US/CAN-Wert 900 mm lautet. Die Normen unterscheiden sich auch hinsichtlich der Objektempfindlichkeit. Während die ISO/EN-Norm 40 mm bis 70 mm zulässt, sind es bei der US/CAN-Norm bis zu 600 mm.

Übergreifanwendungen

Beide Normen stimmen darin überein, dass die Mindesthöhe des niedrigsten Lichtstrahls bei 300 mm liegen muss. Sie unterscheiden sich jedoch hinsichtlich der Mindesthöhe des höchsten Lichtstrahls. Bei der ISO/EN-Norm liegt diese bei 900 mm, bei der US/CAN-Norm bei 1200 mm. Der Wert für den höchsten Lichtstrahl scheint umstritten zu sein. Würde es sich hierbei um eine Durchgriffsanwendung handeln, müsste die Höhe des höchsten Lichtstrahls wesentlich höher sein, um auch einen Bediener in aufrechter Position erkennen zu können. Wenn der Bediener über die Erkennungsebene greifen könnte, gelten die Übergreifkriterien.

Einzelne oder mehrfache Lichtstrahlen

Einfache oder mehrfache separate Lichtstrahlen sind in den ISO/EN-Normen näher beschrieben. Die nachfolgenden Zahlen entsprechen den „praktischen“ Höhen mehrerer Lichtstrahlen über dem Boden. Die Eindringtiefe liegt in den meisten Fällen bei 850 mm und bei Verwendung eines einzelnen Lichtstrahls bei 1200 mm. Im Vergleich dazu wird dies bei der Herangehensweise der US/CAN-Normen durch die Anforderungen für Durchgriffsanwendungen berücksichtigt. Es muss stets berücksichtigt werden, dass ein Bediener über, unter oder um die Einzel- oder Mehrfach-strahlen gelangen kann.

Anzahl der Strahlen	Höhe über dem Boden (mm)	C (mm)
1	750	1200
2	400, 900	850
3	300, 700, 1100	850
4	300, 600, 900, 1200	850

Berechnung der Abstände

Für die normale Annäherung an Lichtgitter liegen die Berechnungen des Sicherheitsabstands bei den ISO/EN- und US/CAN-Normen nahe beieinander, doch es gibt durchaus Unterschiede. Bei der normalen Annäherung an vertikale Lichtgitter, die eine Objektempfindlichkeit von maximal 40 m aufweisen, erfordert die Herangehensweise der ISO/EN-Normen zwei Schritte. Zunächst wird S berechnet, wobei als Geschwindigkeitskonstante 2000 verwendet wird.

S = 2000 x T + 8 x (d -1 4)

Der Mindestabstand für S lautet 100 mm.

Ein zweiter Schritt wird verwendet, wenn der Abstand größer als 500 mm ist. Dann kann der Wert von K auf 1600 reduziert werden. Wenn K = 1600 verwendet wird, entspricht der minimale Wert von S 500 mm.

Die US/CAN-Normen verwenden eine einstufige Herangehensweise: Ds = 1600 x T * Dpf

Dies führt zwischen den Normen zu Unterschieden von über 5 %, wenn die Reaktionszeit unter 560 ms liegt.

Annäherungen

Die meisten Lichtgitter und Scanner sind vertikal (normale Annäherung) oder horizontal (parallele Annäherung) montiert. Diese Montagearten werden nicht als winklig bezeichnet, wenn sie innerhalb von ±5° der beabsichtigten Konstruktion liegen. Wenn der Winkel ±5° überschreitet, müssen die möglichen Risiken (z. B. kürzester Abstand) der vorhersehbaren Annäherung berücksichtigt werden. Im Allgemeinen gelten Winkel von der Referenzebene (z. B. dem Boden), die größer sind als 30°, als normal. Bei kleineren Winkeln geht man von Parallelität aus.

Schaltmatten

Mit Schaltmatten muss für den Sicherheitsabstand die Geschwindigkeit und Schrittgröße des Bedieners berücksichtigt werden. Angenommen, der Bediener läuft über die am Boden montierten Schaltmatten. Der erste Schritt des Bedieners auf der Matte entspricht einem Eindringtiefenfaktor von 1200 mm. Wenn der Bediener eine Plattform betreten muss, kann sich der Eindringtiefenfaktor um einen Faktor von 40 % der Stufenhöhe verringern.

Beispiel

Beispiel: Ein Bediener verwendet eine normale Annäherung an ein 14-mm-Lichtgitter, das an einem Sicherheitsrelais angeschlossen ist, das wiederum an einem DC-Leistungsschütz mit Dioden-Löschglied angeschlossen ist. Die Reaktionszeit des Sicherheitssystems, Tr, liegt bei 20 + 15 + 95 = 130 ms. Die Stoppzeit der Maschine, Ts+Tc, liegt bei 170 ms. Es wird keine Bremsenüberwachung verwendet. Der Wert Dpf entspricht 1 Zoll (25,4 mm), während der Wert C gleich 0 ist. Die Berechnung würde wie folgt aussehen:

Dpf = 3,4 (14–6,875) = 1 Zoll (24,2 mm)

C = 8 (14–14) = 0

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 19,9 Zoll (505 mm)

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18,9 Zoll)

Daher muss der minimale Sicherheitsabstand zwischen Sicherheitslichtgitter und Gefahrenquelle 508 mm betragen, wenn eine Maschine in der ganzen Welt einsetzbar sein soll.

Verhinderung unerwarteten Einschaltens

Viele Normen sehen die Verhinderung des unerwarteten Einschaltens vor. Beispiele hierfür sind ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 und AS 4024.1603. Diese Normen befassen sich alle mit einem Thema: Die primäre Methode zum Verhindern eines unerwarteten Einschaltens ist die Unterbrechung der Spannungsversorgung des Systems und die Verriegelung des Systems im ausgeschalteten Zustand. Zweck dieser Methode ist es, Personen den sicheren Zugang zu den Gefahrenzonen einer Maschine zu ermöglichen.

Verriegelung/Kennzeichnung

Neue Maschinen müssen mit verriegelbaren Vorrichtungen zur Abschaltung der Energieversorgung ausgestattet sein. Die Geräte gelten für alle Energietypen, wie elektrische, hydraulische, pneumatische Energie, Gravitationskraft und Laser. Verriegelung (Lockout) bedeutet, dass eine Vorrichtung zur Trennung der Maschine von der Energiequelle mit einer Sperre versehen wird. Die Verriegelung darf nur von ihrem Eigentümer oder von einem Vorgesetzten unter kontrollierten Bedingungen entfernt werden. Wenn mehrere Personen an der Maschine arbeiten sollen, muss jede Person eine eigene Verriegelung an den Vorrichtungen zur Abschaltung der Energieversorgung anbringen. Jede Verriegelung muss für ihren Eigentümer identifizierbar sein.

In den USA ist bei älteren Maschinen die Kennzeichnung (Tagout) eine Alternative zur Verriegelung (Lockout), wenn an diesen Maschinen keine verriegelbaren Geräte installiert wurden. In diesem Fall wird die Maschine ausgeschaltet und ein Etikett warnt alle Personen, die Maschine nicht in Betrieb zu nehmen, solange das Etikett angebracht ist. Seit 1990 müssen alle Maschinen, an denen Änderungen vorgenommen werden, mit einem verriegelbaren Gerät zur Abschaltung der Energieversorgung nachgerüstet werden.

Ein Gerät zur Abschaltung der Energieversorgung ist ein mechanisches Gerät, das die Übertragung oder die Freisetzung von Energie physisch verhindert. Diese Geräte können z. B. ein Leistungsschalter, ein Trennschalter, ein manuell betätigter Schalter, eine Stecker/Buchse-Kombination oder ein manuell betätigtes Ventil sein. Geräte zur Abschaltung der Energieversorgung müssen alle nicht geerdeten Versorgungsleiter schalten, wobei kein Pol unabhängig arbeiten darf.

Zweck von Verriegelung und Kennzeichnung ist die Verhinderung eines unerwarteten Anlaufens der Maschine. Ein unerwartetes Anlaufen kann verschiedene Ursachen haben: ein Fehler des Steuerungssystems, eine falsche Aktion einer Anlaufsteuerung, eines Sensors, eines Schützes oder eines Ventils, die Wiederherstellung der Stromversorgung nach einer Unterbrechung und sonstige interne sowie externe Einflüsse. Nach Abschluss des Verriegelungs-/Kennzeichnungsvorgangs muss sichergestellt werden, dass die Energie abgeleitet wird.

Sicherheits-Trennsysteme

Sicherheits-Trennsysteme schalten eine Maschine ordnungsgemäß ab und bieten zudem eine einfache Möglichkeit, die Spannungsversorgung einer Maschine abzuschalten. Dieses Konzept eignet sich hervorragend für größere Maschinen und Fertigungssysteme, ins-

besondere, wenn sich mehrere Energiequellen auf einem Zwischengeschoss oder an weit entfernten Standorten befinden.

Lasttrenner

Für die lokale Trennung elektrischer Geräte können Schalter direkt vor dem von der Energieversorgung zu trennenden und gegen versehentliches Wiedereinschalten zu verriegelnden Gerät positioniert werden. Die Lastschalter der Serie 194E sind Beispiele für ein Produkt, das sowohl für Trennung als auch Verriegelung sorgen kann.

Schlüsseltransfersysteme

Schlüsseltransfersysteme sind eine weitere Möglichkeit zum Realisieren eines Verriegelungssystems. Viele Schlüsseltransfersysteme basieren auf einem Gerät zur Abschaltung der Energieversorgung. Beim Deaktivieren des Schalters mit dem Primärschlüssel wird die elektrische Energieversorgung der Maschine zu allen nicht geerdeten Versorgungsleitern gleichzeitig unterbrochen. Der Primärschlüssel kann anschließend abgezogen und zu einer Stelle gebracht werden, an der der Maschinenzugriff erforderlich ist. Verschiedene Komponenten können hinzugefügt werden, um komplexere Verriegelungen zu ermöglichen.

Alternative Maßnahmen anstelle von Verriegelung

Verfahren zur Verriegelung und Kennzeichnung müssen während Wartungs- und Instandhaltungsarbeiten an den Maschinen verwendet werden. Maschineneingriffe während des normalen Produktionsbetriebs werden durch Schutzeinrichtungen verhindert. Der Unterschied zwischen Wartungs-/Instandhaltungsarbeiten und dem normalen Produktionsbetrieb ist nicht immer eindeutig.

Einige kleinere Anpassungen und Wartungsarbeiten, die während des normalen Produktionsbetriebs vorgenommen werden müssen, erfordern nicht unbedingt das Abschalten und Verriegeln der Energieversorgung der Maschine. Beispiele hierfür sind das Be- und Entladen von Material, geringfügige Werkzeugwechsel und -justierungen, Schmierzyklen im Rahmen der Wartung und das Entfernen von Ausschuss. Hierbei handelt es sich um wiederholt auftretende Routineaufgaben, die für die Verwendung der Anlagen in der Produktion unabdingbar sind. Die Arbeiten werden mithilfe alternativer Maßnahmen wie zum Beispiel Schutzeinrichtungen vorgenommen, welche ausreichenden Schutz bieten. Zu den Schutzeinrichtungen gehören Geräte wie verriegelte Schutztüren, Lichtgitter und Schaltmatten. Wenn zudem geeignete Sicherheitslogikgeräte und -ausgangsgeräte eingesetzt werden, besteht für die Bediener während der normalen Produktion und bei kleineren Wartungsarbeiten sicherer Zugang zu den Gefahrenzonen der Maschinen.

Sicherheitsbezogene Steuerungssysteme

Einführung

Was ist ein sicherheitsbezogenes Steuerungssystem (oft auch abgekürzt mit SRCS – Safety-Related Control System)? Es handelt sich um den Teil des Steuerungssystems einer Maschine, der das Auftreten gefährlicher Zustände verhindert. Das System kann separat ausgeführt oder in das normale Steuerungssystem einer Maschine integriert sein.

Die Komplexität reicht von einfachen Systemen (z. B. Schutztür-Verriegelungsschalter und Not-Halt-Schalter in Reihe geschaltet mit der Steuerspule eines Leistungsschützes) bis hin zu Verbundsystemen, in denen sowohl einfache als auch komplexe Geräte mittels Software und Hardware kommunizieren.

Sicherheitsbezogene Steuerungssysteme wurden zum Ausführen von Sicherheitsfunktionen entwickelt. Ein sicherheitsbezogenes Steuerungssystem muss unter allen vorhersehbaren Bedingungen korrekt funktionieren. Was also ist eine Sicherheitsfunktion? Wie wird ein System ausgelegt, um dies zu erreichen? Wie wird die richtige Konstruktion nachgewiesen?

Sicherheitsfunktion

Eine Sicherheitsfunktion wird durch die sicherheitsbezogenen Teile des Steuerungssystems der Maschine realisiert, um die Anlage hinsichtlich einer bestimmten Gefahr in einem sicheren Zustand unter Kontrolle zu halten. Der Ausfall der Sicherheitsfunktion kann zur unmittelbaren Erhöhung der Risiken bei der Verwendung der Anlage führen, also zu einer gefährlichen Bedingung.

Eine Maschine muss mindestens eine „Gefahrenquelle“ aufweisen, da es sich anderenfalls nicht um eine Maschine handelt. Eine „gefährliche Bedingung“ besteht dann, wenn eine Person einer Gefahr ausgesetzt wird. Eine solche Bedingung impliziert nicht die tatsächliche Verletzung der Person. Die der Gefahr ausgesetzte Person kann in der Lage sein, die Gefahr zu erkennen und eine Verletzung zu vermeiden. Die der Gefahr ausgesetzte Person ist eventuell jedoch nicht in der Lage, die Gefahr zu erkennen, oder die Gefahr kann erst durch ein unerwartetes Anlaufen der Maschine entstehen. Die Hauptaufgabe für den Entwickler des Sicherheitssystems besteht darin, gefährliche Bedingungen zu vermeiden und ein unerwartetes Anlaufen der Maschine zu verhindern.

Die Sicherheitsfunktion kann auch oft mit Anforderungen für mehrere Teile beschrieben werden. Beispielsweise besteht die Sicherheitsfunktion, die durch eine Schutztür initiiert wird, aus drei Teilen:

1. Die gefährlichen Vorgänge, vor denen die Schutztür schützt, können erst ausgelöst werden, wenn die Schutztür geschlossen ist.

2. Beim Öffnen der Schutztür wird der gefährliche Vorgang gestoppt, sofern er aktiv ist.

3. Beim Schließen der Schutztür wird der gefährliche Vorgang, vor dem die Schutztür schützt, nicht wieder gestartet.

Wird eine Sicherheitsfunktion für eine bestimmte Anwendung formuliert, muss das Wort „Gefahr“ oder „gefährlicher Vorgang“ durch die Beschreibung der speziellen Gefahr ersetzt werden. Die Gefahr darf nicht mit der Folge der Gefahr verwechselt werden. Quetschungen, Schnittwunden und Verbrennungen sind Folgen einer Gefahr. Beispiele für eine Gefahr sind Motoren, Stempel, Messer, Lötlampen, Pumpen, Laser, Roboter, Greifer, Magnetspulen, Ventile, andere Aktorentypen oder eine mechanische Gefahr durch Gravitation.

Bei der Erörterung von Sicherheitssystemen wird die Formulierung „wenn oder bevor die Sicherheitsfunktion angefordert wird“ verwendet. Was versteht man unter dem Anfordern der Sicherheitsfunktion? Beispiele hierfür sind das Öffnen einer Schutztür, die Unterbrechung eines Lichtgitters, das Treten auf eine Schaltmatte oder das Betätigen eines Not-Halt-Schalters. Ein Bediener fordert an, dass der gefährliche Vorgang entweder gestoppt wird oder ausgeschaltet bleibt, sofern er bereits gestoppt wurde.

Die sicherheitsbezogenen Teile des Steuerungssystems der Maschine führen die Sicherheitsfunktion aus. Die Sicherheitsfunktion wird nicht von einem einzelnen Gerät, z. B. nur von der Schutztür, ausgeführt. Die Verriegelung der Schutztür sendet einen Befehl an ein Logikgerät, das wiederum einen Aktor deaktiviert. Die Sicherheitsfunktion beginnt mit dem Befehl und endet mit der Realisierung.

Das Sicherheitssystem muss eine gewisse Integritätsstufe umfassen, die den Risiken der Maschine angemessen ist. Höhere Risiken erfordern auch höhere Integritätsstufen, um die Leistungsfähigkeit der Sicherheitsfunktion zu gewährleisten. Maschinensicherheitssysteme können abhängig von ihrer Fähigkeit, die Leistungsfähigkeit ihrer Sicherheitsfunktion zu gewährleisten, (also abhängig von ihrem funktionalen Sicherheits-Integritätslevel) klassifiziert werden.

Funktionale Sicherheit des Steuerungssystems

Wichtig: *Die in diesem Abschnitt berücksichtigten Normen und Anforderungen sind relativ neu. Einige Aspekte sind noch in Arbeit, insbesondere wenn es um die Verdeutlichung und Kombination einiger dieser Normen geht. Daher können einige Details auf diesen Seiten eventuell noch geändert werden. Aktuelle Informationen finden Sie unter folgender Adresse: http://www.ab.com/safety.*

Was ist funktionale Sicherheit?

Funktionale Sicherheit ist der Teil der allgemeinen Sicherheit, der vom ordnungsgemäßen Funktionieren des Prozesses oder der Anlage als Reaktion auf deren Eingänge abhängt. IEC TR 61508-0 verdeutlicht den Sinn der funktionalen Sicherheit anhand des folgenden Beispiels. „Ein Beispiel für funktionale Sicherheit ist ein Übertemperatur-Schutzgerät mit einem Wärmesensor in den Wicklungen eines Elektromotors, das ein Abschalten des Motors veranlasst, bevor dieser überhitzt. Dagegen ist die Bereitstellung einer speziellen Isolierung, die hohen Temperaturen standhält, kein Beispiel für funktionale Sicherheit (auch wenn es sich weiterhin um ein

Beispiel für Sicherheit handelt und die Isolierung vor exakt derselben Gefahr schützen könnte).“ In einem weiteren Beispiel werden fest installierte Schutzvorrichtungen mit verriegelten Schutzvorrichtungen verglichen. Die fest installierte Schutzvorrichtung bietet keine „funktionale Sicherheit“, selbst wenn sie als verriegelte Tür den Zugang zur selben Gefahr verhindert. Die verriegelte Tür ist ein Beispiel für funktionale Sicherheit. Wenn die Sicherheitsvorrichtung geöffnet wird, dient die Verriegelung als „Eingabe“ in das System, die gewährleistet, dass ein sicherer Zustand erzielt wurde. Auf ähnliche Weise werden persönliche Schutzausrüstungen als Schutzmaßnahme für eine höhere Sicherheit des Personals verwendet. Persönliche Schutzausrichtung stellt keine funktionale Sicherheit dar.

Funktionale Sicherheit wurde als Begriff mit der Norm IEC 61508:1998 eingeführt. Seitdem wurde der Begriff manchmal ausschließlich mit programmierbaren Sicherheitssystemen assoziiert. Dies ist jedoch eine falsche Auffassung. Funktionale Sicherheit deckt eine große Bandbreite von Geräten ab, die zum Erstellen von Sicherheitssystemen verwendet werden. Geräte wie Verriegelungen, Lichtgitter, Sicherheitsrelais, Sicherheits-SPS, Sicherheitsschütze und Sicherheitsantriebe sind miteinander verbunden, um ein Sicherheitssystem zu bilden, das eine bestimmte sicherheitsbezogene Funktion ausführt. Hierbei handelt es sich um funktionale Sicherheit. Daher ist die funktionale Sicherheit eines elektrischen Steuerungssystems für die Kontrolle von Gefahren, die von beweglichen Teilen einer Maschine ausgehen, äußerst relevant.

Zwei Anforderungstypen sind erforderlich, um die funktionale Sicherheit zu erzielen:

- Sicherheitsfunktion und
- Sicherheitsintegrität

Die Risikobeurteilung spielt eine wichtige Rolle bei der Entwicklung der Anforderungen an die funktionale Sicherheit. Mit der Aufgaben- und Gefahrenanalyse werden die funktionalen Anforderungen an die Sicherheit abgeleitet (also die Sicherheitsfunktion). Aus der Risikoquantifizierung ergeben sich die Anforderungen an die Sicherheitsintegrität, d. h. die Stufe der Sicherheitsintegrität (SIL) oder der Performance Level (PL).

Vier der bedeutendsten Normen zur funktionalen Sicherheit von Steuerungssystemen für Maschinenanlagen sind:

1. **IEC/EN 61508** „Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“

   Diese Norm enthält die Anforderungen und Voraussetzungen für die Entwicklung komplexer elektronischer und programmierbarer Systeme und Subsysteme. Die Norm ist generisch, d. h. sie ist nicht auf den Maschinensektor beschränkt.

2. **IEC/EN 62061** „Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“

Bei dieser Norm handelt es sich um die maschinenspezifische Realisierung von IEC/EN 61508. Diese Norm definiert die Anforderungen für die Entwicklung der Systemebene aller sicherheitsbezogenen elektrischen Steuerungssysteme für alle Maschinentypen sowie für die Entwicklung nicht komplexer Subsysteme oder Geräte. Sie fordert, dass komplexe oder programmierbare Subsysteme der Norm IEC/EN 61508 entsprechen.

3. **EN ISO 13849-1:2008** „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“

   Diese Norm soll einen direkten Übergangspfad von den Kategorien der vorherigen Norm EN 954-1 bereitstellen.

4. **IEC 61511** „Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie“

   Diese Norm ist die speziell für die Prozessindustrie implementierte Version der Norm IEC/EN 61508.

Die Normen zur funktionalen Sicherheit stellen einen großen Schritt über die vertrauten, bestehenden Anforderungen hinaus dar, wie z. B. die Steuerungszuverlässigkeit und das Kategoriensystem der vorherigen Norm ISO 13849-1:1999 (EN 954-1:1996).

Die neue Version der Norm EN ISO 13849-1 verwendet das Konzept der funktionalen Sicherheit und führt neue Terminologie und Anforderungen ein. Sie weist bedeutende Ergänzungen und Unterschiede im Vergleich zur alten Norm EN 954-1 (ISO 13849-1:1999) auf. In diesem Abschnitt wird auf die aktuelle Version als EN ISO 13849-1 verwiesen. (EN ISO 13849-1:2008 enthält denselben Text wie die Norm ISO 13849-1:2006).

IEC/EN 62061 und EN ISO 13849-1:2008

Die Normen IEC/EN 62061 und EN ISO 13849-1 decken beide sicherheitsbezogene elektrische Steuerungssysteme ab. Sie sollen zu einer einzigen Norm mit gemeinsamer Terminologie kombiniert werden. Beide Normen führen zu den gleichen Ergebnissen, wenden aber unterschiedliche Methoden an. Sie sollen Anwendern die Möglichkeit geben, die Methode auszuwählen, die sich für ihre Situation am besten eignet. Ein Anwender kann sich für eine der beiden Normen entscheiden, die beide unter der EU-Maschinenrichtlinie harmonisiert wurden.

Die Ergebnisse beider Normen sind vergleichbare Stufen der Sicherheitsleistung oder -integrität. Die Unterschiede der Methodiken der Normen sind auf die jeweiligen Anwender abgestimmt.

Die Methodiken der Norm IEC/EN 62061 sollen komplexe Sicherheitsfunktionalität ermöglichen, die durch zuvor unkonventionelle Systemarchitekturen realisiert werden können. Die Methodiken der Norm EN ISO 13849-1 sollen eine direkte und weniger komplizierte Anleitung

für eine konventionellere Sicherheitsfunktionalität zur Verfügung stellen, die durch konventionelle Systemarchitekturen realisiert wird.

Ein wichtiges Unterscheidungsmerkmal dieser beiden Normen ist die Anwendbarkeit auf verschiedene Technologien. IEC/EN 62061 ist auf elektrische Systeme beschränkt. EN ISO 13849-1 kann auf pneumatische, hydraulische, mechanische und elektrische Systeme angewandt werden.

Gemeinsamer technischer Bericht zu IEC/EN 62061 und EN ISO 13849-1

Von den Institutionen IEC und ISO wurde ein gemeinsamer Bericht ausgearbeitet, der Anwendern die Verwendung beider Normen erleichtern soll.

Er erläutert die Beziehung der beiden Normen und verdeutlicht, wie die Äquivalenz zwischen PL (Performance Level) der Norm EN ISO 13849-1 und SIL (Safety Integrity Level) der Norm IEC/EN 62061 auf System- und Subsystemebene hergestellt werden kann.

Zur Veranschaulichung, dass aus beiden Normen äquivalente Ergebnisse resultieren, wird in dem Bericht ein Beispielsicherheitssystem aufgeführt, das gemäß den Methoden beider Normen berechnet wurde. Der Bericht verdeutlicht verschiedene Aspekte, die unterschiedlich interpretiert wurden. Zu den bedeutendsten Aspekten zählt wahrscheinlich der Fehlerausschluss.

Wenn PLe für die Implementierung einer Sicherheitsfunktion durch ein sicherheitsbezogenes Steuerungssystem erforderlich ist, darf man sich im Allgemeinen nicht allein auf Fehlerausschlüsse verlassen, um diesen Performance Level zu erreichen. Dies hängt von der verwendeten Technologie und der vorgesehenen Betriebsumgebung ab. Daher ist es wichtig, dass der Entwickler bei der Verwendung von Fehlerausschlüssen umso vorsichtiger vorgeht, je höher die PL-Anforderung ist.

Im Allgemeinen kann die Verwendung von Fehlerausschlüssen nicht auf die mechanischen Aspekte elektromechanischer Positionsschalter und manuell betätigter Schalter (z. B. Not-Halt-Geräte) angewandt werden, um PLe bei der Konstruktion eines sicherheitsbezogenen Steuerungssystems zu erzielen. Fehlerausschlüsse, die auf bestimmte mechanische Fehlerzustände angewandt werden können (z. B. Verschleiß/Korrosion, Brüche), sind in Tabelle A.4 der Norm ISO 13849-2 beschrieben.

Beispielsweise muss ein Türzuhaltungssystem, das PLe erzielen muss, über eine minimale Fehlertoleranz von 1 (z. B. zwei konventionelle mechanische Positionsschalter) verfügen, um diesen Performance Level zu erreichen, da normalerweise der Ausschluss von Fehlern wie gebrochene Schalterbetätiger nicht zu rechtfertigen ist. Es ist jedoch eventuell akzeptabel, Fehler auszuschließen, wie z. B. einen Verdrahtungskurzschluss innerhalb eines Schaltschranks, der in Übereinstimmung mit relevanten Industrienormen entwickelt wurde.

SIL und IEC/EN 62061

Die Norm IEC/EN 62061 beschreibt das zu mindernde Risiko und die Fähigkeit eines Steuerungssystems, dieses Risiko im Sinne des SIL (Safety Integrity Level) zu mindern. Drei SILs werden im Maschinensektor verwendet, wobei SIL 1 der niedrigste und SIL 3 der höchste Sicherheits-Integritätslevel ist.

Da der Begriff SIL in anderen Industriezweigen wie z. B. Petrochemie, Stromerzeugung und Schienenverkehr auf dieselbe Weise angewandt wird, ist IEC/EN 62061 äußerst nützlich, wenn Maschinen in diesen Branchen eingesetzt werden. Risiken von größerem Ausmaß können in anderen Sektoren auftreten, wie z. B. der Prozessindustrie. Aus diesem Grund umfassen die Norm IEC 61508 und die für den Prozesssektor spezifische Norm IEC 61511 den Sicherheits-Integritätslevel SIL 4.

Ein Sicherheits-Integritätslevel (SIL) bezieht sich auf eine Sicherheitsfunktion. Die Subsysteme, aus denen das System besteht, das die Sicherheitsfunktion realisiert, müssen über eine entsprechende SIL-Eignung verfügen. Dies wird manchmal auch als SIL Claim Limit (SIL CL) bezeichnet, also als SIL-Anspruchsgrenze. Bevor die Norm IEC/EN 62061 richtig angewandt werden kann, muss sie vollständig und detailliert überprüft werden.

PL und EN ISO 13849-1:2008

EN ISO 13849-1:2008 verwendet den Begriff SIL nicht. Stattdessen wird der Begriff PL (Performance Level) verwendet. Eine Verbindung zwischen PL und SIL gibt es in vielerlei Hinsicht. Es gibt fünf Performance Levels, von denen PLa die niedrigste und PLe die höchste ist.

Vergleich von PL und SIL

Diese Tabelle veranschaulicht die ungefähre Beziehung zwischen PL und SIL, wenn diese auf typische Schaltkreisstrukturen angewandt werden.

PL (Performance Level)	PFHd (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)	SIL (Safety Integrity Level)
a	$\geq 10^{-5}$ bis $<10^{-4}$	Keine
b	$\geq 3 \times 10^{-6}$ bis $<10^{-5}$	1
c	$\geq 10^{-6}$ bis $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ bis $<10^{-6}$	2
e	$\geq 10^{-8}$ bis $<10^{-7}$	3

Ungefähre Entsprechung von PL und SIL

***WICHTIG:** Die oben abgebildete Tabelle soll eine allgemeine Anleitung zur Verfügung stellen und darf NICHT zu Konvertierungszwecken verwendet werden. Es müssen die vollständigen Anforderungen der Normen berücksichtigt werden.*

Systemaufbau gemäß EN ISO 13849 und SISTEMA

Bevor die Norm EN/ISO 13849-1:2008 richtig angewandt werden kann, muss sie vollständig und detailliert überprüft werden. Es folgt eine kurze Übersicht:

Diese Norm stellt Anforderungen für die Entwicklung und Integration sicherheitsbezogener Teile des Steuerungssystems zur Verfügung, einschließlich einiger Softwareaspekte. Die Norm bezieht sich auf ein sicherheitsbezogenes System, kann jedoch auch auf die Komponenten-teile des Systems angewandt werden.

PL-Berechnungstool der SISTEMA-Software

SISTEMA ist ein Software-Tool für die Implementierung von EN ISO 13849-1. Es sorgt für eine erheblich einfachere Implementierung der Norm.

SISTEMA steht für „Safety Integrity Software Tool for the Evaluation of Machine Applications“ (Software-Tool zur Bewertung der Sicherheit von Maschinenanwendungen). Das Software-Tool wurde vom Berufsgenossenschaftlichen Institut für Arbeitsschutz (BGIA) in Deutschland entwickelt und steht kostenlos zur Verfügung. Es erfordert die Eingabe verschiedener Daten zur funktionalen Sicherheit, die weiter hinten in diesem Abschnitt beschrieben sind.

Die Daten können manuell oder automatisch mithilfe einer SISTEMA-Datenbibliothek des Herstellers eingegeben werden.

Die SISTEMA-Datenbibliothek von Rockwell Automation steht auf der folgenden Webseite zum Herunterladen zur Verfügung. Dort befindet sich auch ein Link zur SISTEMA-Download-Webseite: *www.discoverrockwellautomation.com/safety*

EN ISO 13849-1 – Überblick

Diese Norm gilt für die unterschiedlichsten Anwendungen und kann auf alle Technologien angewandt werden, wie z. B. elektrische, hydraulische, pneumatische und mechanische Systeme. Zwar kann die Norm ISO 13849-1 auch auf komplexe Systeme angewandt werden, doch sie verweist den Leser auf IEC 62061 und IEC 61508, wenn es um komplexe, softwareintegrierte Systeme geht.

Im Folgenden sind die grundlegenden Unterschiede zwischen der alten Norm EN 954-1 und der neuen Norm EN ISO 13849-1 aufgeführt. Die Ergebnisse der alten Norm waren Kategorien [B, 1, 2, 3 oder 4]. Die Ergebnisse der neuen Norm sind Performance Level [PL a, b, c, d oder e]. Das Konzept der Kategorien wird beibehalten, doch es müssen zusätzliche Anforderungen erfüllt werden, bevor ein System eine PL-Klassifizierung erhält.

Die Anforderungen können auf einfache Weise wie folgt aufgelistet werden:

- Architektur des Systems. Im Grunde genommen wird mit dieser erfasst, was in der Zwischenzeit als Kategorien gebräuchlich ist.
- Daten zur Zuverlässigkeit sind für die einzelnen Teile des Systems erforderlich.
- Der Diagnosedeckungsgrad (DC – Diagnostic Coverage) des Systems ist erforderlich. Dieser stellt effektiv das Ausmaß der Fehlerüberwachung im System dar.
- Schutz vor Fehlern mit gemeinsamer Ursache
- Schutz vor systematischen Fehlern
- Sofern relevant, spezielle Anforderungen an die Software

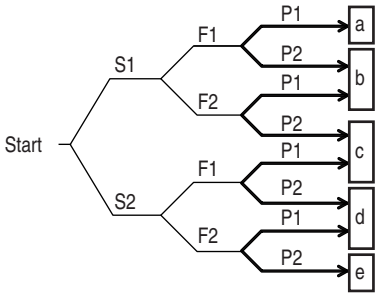
Später werden diese Faktoren näher beschrieben. Doch zuvor wollen wir uns mit den grundlegenden Absichten und Prinzipien der gesamten Norm vertraut machen. Denn die Details lassen sich erst dann erschließen, wenn Sie die eigentlichen Ziele und Gründe dieser Norm verstanden haben.

Warum ist die neue Norm überhaupt erforderlich? Es ist offensichtlich, dass sich die in Maschinensicherheitssystemen eingesetzte Technologie in den letzten zehn Jahren weiterentwickelt und enorm verändert hat. Bis vor kurzem waren Sicherheitssysteme von „einfachen“ Geräten mit äußerst gut vorhersehbaren und berechenbaren Fehlermodi abhängig. In der letzten Zeit werden zunehmend komplexe elektronische und programmierbare Geräte in Sicherheitssystemen eingesetzt. So entstanden Vorteile hinsichtlich Kosten, Flexibilität und Kompatibilität, doch es bedeutete auch, dass die bisherigen Normen nicht mehr ausreichend waren. Um festzustellen, ob ein Sicherheitssystem gut genug ist, müssen wir mehr darüber wissen. Daher verlangt die neue Norm zusätzliche Informationen. Da Sicherheitssysteme angefangen haben, mit einer Art „Blackbox“-Ansatz zu arbeiten, sind wir stärker davon abhängig, dass diese mit den Normen übereinstimmen. Daher müssen diese Normen die Technologie angemessen hinterfragen. Um diese Anforderung zu erfüllen, müssen sie die grundlegenden Faktoren Zuverlässigkeit, Fehlererkennung, architekturbezogene und systematische Integrität abdecken. Dies ist die Absicht der Norm EN ISO 13849-1.

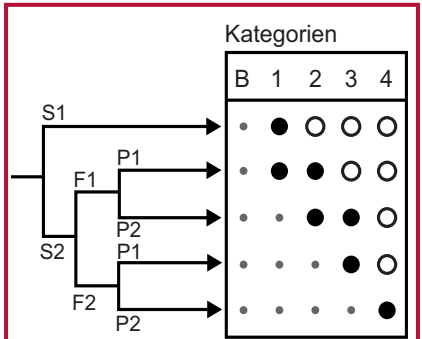
Um den roten Faden durch die Norm zu erkennen, müssen zwei grundsätzlich verschiedene Anwendertypen berücksichtigt werden: der Entwickler der sicherheitsbezogenen Subsysteme und die Entwickler der sicherheitsbezogenen Systeme. Im Allgemeinen hat es der Entwickler der Subsysteme (in der Regel ein Komponentenhersteller) mit einer wesentlich höheren Komplexität zu tun. Er muss die erforderlichen Daten bereitstellen, damit der Systementwickler sicherstellen kann, dass die Integrität des Subsystems für das System ausreichend ist. Dies erfordert in der Regel einige Tests, Analysen und Berechnungen. Die Ergebnisse werden in Form der Daten ausgedrückt, die von der Norm gefordert werden.

Der Systementwickler (in der Regel ein Maschinenentwickler oder Integrator) verwendet die Daten des Subsystems, um einige relativ unkomplizierte Berechnungen durchzuführen, mit denen der allgemeine Performance Level (PL) des Systems bestimmt werden kann.

Mithilfe von PLr wird angegeben, welchen Performance Level die Sicherheitsfunktion erfordert. Zum Bestimmen des PLr stellt die Norm ein Risikodiagramm zur Verfügung, in das die Anwendungsfaktoren „Schwere der Verletzungen“, „Häufigkeit des Aufenthalts im Gefahrenbereich“ und „Möglichkeit der Vermeidung“ eingegeben werden.



Risikodiagramm aus Anhang A der Norm EN ISO 13849-1



Risikodiagramm aus Anhang B der Norm EN 945-1

Das Ergebnis ist der PLr. Anwender der alten Norm EN 954-1 werden mit diesem Ansatz vertraut sein, sollten jedoch beachten, dass die S1-Linie nun untergliedert ist, was im alten Risikodiagramm nicht der Fall war. Beachten Sie, dass dies möglicherweise eine erneute Prüfung der Integrität der Sicherheitsmaßnahmen erforderlich macht, die für niedrigere Risikostufen erforderlich sind.

Es muss jedoch noch ein äußerst wichtiger Aspekt abgedeckt werden. Aus der Norm ist nun bekannt, wie gut das System sein muss und wie bestimmt werden kann, wie gut es ist. Wir wissen jedoch nicht, wie das System arbeiten muss. Wir müssen festlegen, worum es sich bei der Sicherheitsfunktion handelt. Natürlich muss die Sicherheitsfunktion für die Aufgabe geeignet sein. Wie können wir dies sicherstellen? Wie kann uns die Norm dabei helfen?

Es muss unbedingt erkannt werden, dass die erforderliche Funktionalität nur bestimmt werden kann, wenn die maßgeblichen Merkmale der tatsächlichen Anwendung berücksichtigt werden. Dies kann als Entwicklungsphase des Sicherheitskonzepts betrachtet werden. Sie lässt sich nicht vollständig durch die Norm abdecken, da die Norm nicht alle Merkmale einer bestimmten Anwendung kennt. Dies gilt oft für Maschinenbauer, die die Maschine zwar herstellen, jedoch nicht unbedingt wissen, unter welchen genauen Bedingungen die Maschine eingesetzt wird.

Die Norm gibt einige Hilfestellungen, da sie viele gängige Sicherheitsfunktionen auflistet (z. B. durch eine Schutzeinrichtung ausgelöste sicherheitsbezogene Stoppfunktion, Mutingfunktion, Start-/Neustartfunktion) und einige Anforderungen nennt, die diesen normalerweise zugeordnet sind. Andere Normen wie EN ISO 12100: „Allgemeine Gestaltungsleitsätze“ und EN ISO 14121: „Risikobeurteilung“ werden für die Verwendung in dieser Phase empfohlen. Außerdem steht eine Vielzahl maschinenspezifischer Normen mit Lösungen für bestimmte Maschinen zur Verfügung. Innerhalb der europäischen EN-Normen werden sie Normen vom Typ C genannt und manche von ihnen verfügen über exakte Äquivalente in den ISO-Normen.

Nun sollte klar sein, dass die Entwicklungsphase des Sicherheitskonzepts vom Maschinentyp und von den Merkmalen der Anwendung und Umgebung abhängt, in der die Maschine eingesetzt wird. Nur wenn der Maschinenbauer diese Faktoren kennt, kann er das Sicherheitskonzept entwickeln. Die beabsichtigten (also vorauszusehenden) Bedingungen der Anwendung müssen im Benutzerhandbuch angegeben werden. Der Anwender der Maschine muss überprüfen, ob sie den tatsächlichen Einsatzbedingungen entsprechen.

Nun steht also eine Beschreibung der Sicherheitsfunktion zur Verfügung. Aus Anhang A der Norm ergibt sich auch der erforderliche Performance Level (PLr) für die sicherheitsbezogenen Teile des Steuerungssystems (SRP/CS), die für die Implementierung dieser Funktionalität verwendet werden. Jetzt muss das System entwickelt werden. Gleichzeitig ist sicherzustellen, dass es mit den Anforderungen für PLr übereinstimmt.

Einer der wichtigsten Faktoren für die Entscheidung, welche Norm verwendet wird [EN ISO 13849-1 oder EN/IEC 62061], ist die Komplexität der Sicherheitsfunktion. In den meisten Fällen ist die Sicherheitsfunktion für Maschinen relativ einfach, sodass häufig EN ISO 13849-1 Anwendung findet. Für die Beurteilung des PL werden Daten zu Zuverlässigkeit, Diagnosedeckungsgrad (DC), Systemarchitektur (Kategorie), Ausfällen aufgrund gemeinsamer Ursache und, sofern relevant, Anforderungen an die Software verwendet.

Hierbei handelt es sich um eine vereinfachte Beschreibung, die lediglich einen Überblick bieten soll. Es müssen unbedingt alle Bestimmungen im Text der Norm angewandt werden. Für all dies erhalten Sie eine Hilfestellung. Das Software-Tool SISTEMA kann Sie bei den Dokumentations- und Berechnungsaspekten unterstützen. Darüber hinaus erstellt das Tool eine Akte mit der technischen Dokumentation.

Zum Zeitpunkt der Drucklegung dieser Publikation ist SISTEMA auf Deutsch und Englisch erhältlich. In naher Zukunft werden auch andere Sprachen zur Verfügung stehen. Das Berufsgenossenschaftliche Institut für Arbeitsschutz (BGIA), das SISTEMA entwickelt hat, ist ein in Deutschland ansässiges renommiertes Forschungs- und Prüfinstitut. Es ist vor allem an der Lösung wissenschaftlicher und technischer Probleme beteiligt, die sich auf die Sicherheit im Zusammenhang mit der gesetzlichen Unfallversicherung und -verhinderung in Deutschland beziehen. Es arbeitet eng mit Gesundheits- und Sicherheitsbehörden aus über 20 Ländern zusammen. Experten des BGIA waren zusammen mit ihren BG-Kollegen maßgeblich am Entwurf der Normen EN ISO 13849-1 und IEC/EN 62061 beteiligt.

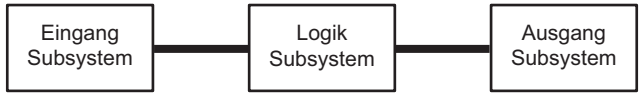
Die „Bibliothek“ mit Sicherheitskomponentendaten von Rockwell Automation, die mit SISTEMA verwendet werden kann, finden Sie unter der folgenden Adresse:

www.discoverrockwellautomation.com/safety

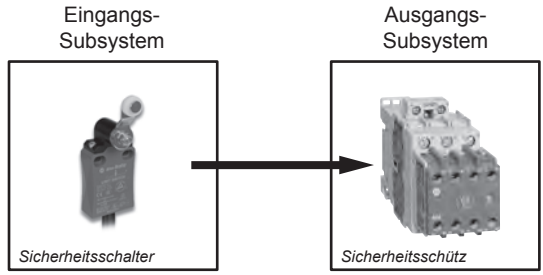
Ganz gleich, auf welche Weise die Berechnung des PL erfolgt, es muss unbedingt von der richtigen Grundlage ausgegangen werden. Zunächst muss das System auf dieselbe Weise betrachtet werden wie dies die Norm tut – also fangen wir damit an.

Systemstruktur

Systeme lassen sich stets in grundlegende Systemkomponenten oder „Subsysteme“ unterteilen. Jedes Subsystem verfügt über seine eigene diskrete Funktion. Die meisten Systeme können in drei Basisfunktionen unterteilt werden: Eingang, Logik/Steuerung (einfache Systeme verfügen gegebenenfalls nicht über die Logikfunktion) und ein Ausgang. Die Komponentengruppen, welche diese Funktionen implementieren, sind die Subsysteme.

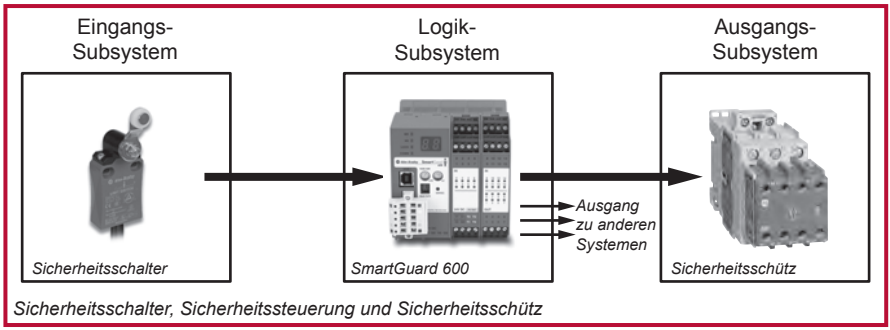


Systeme lassen sich stets in grundlegende Systemkomponenten oder „Subsysteme“ unterteilen. Jedes Subsystem führt seine eigene diskrete Funktion aus. Die meisten Systeme können in drei Basisfunktionen unterteilt werden: Eingang, Logik/Steuerung (einfache Systeme verfügen gegebenenfalls nicht über die Logikfunktion) und ein Ausgang. Die Komponentengruppen, die diese Funktionen implementieren, sind die Subsysteme.



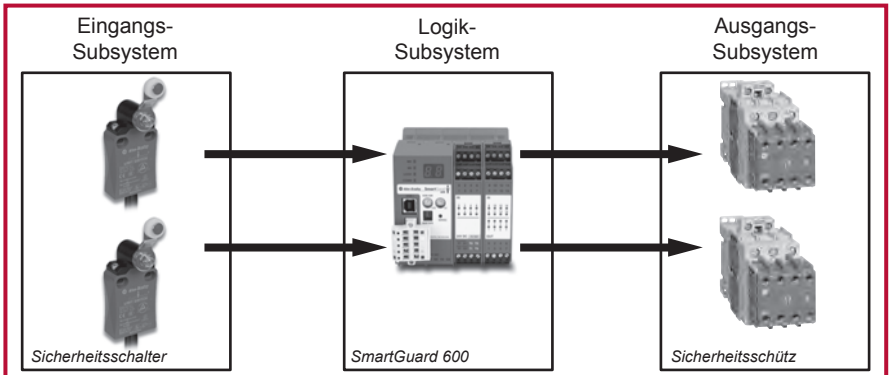
Sicherheitsschalter und Sicherheitsschütz

Die Abbildung oben zeigt ein Beispiel für ein einfaches einkanaliges elektrisches System, das lediglich Eingangs- und Ausgangssubsysteme beinhaltet.



Sicherheitsschalter, Sicherheitssteuerung und Sicherheitsschütz

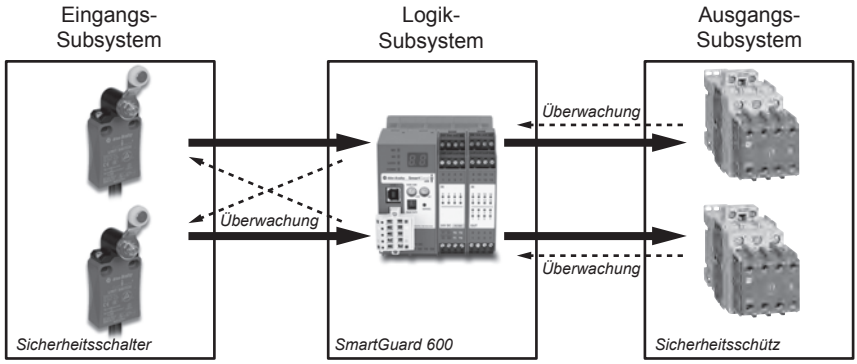
Dieses System ist etwas komplexer: Hier ist auch Logik erforderlich. Die Sicherheitssteuerung selbst ist intern fehlertolerant (z. B. zweikanalig), das Gesamtsystem ist jedoch weiterhin auf Einkanalstatus beschränkt, da es über nur einen Sicherheitsschalter und ein Sicherheitsschütz verfügt.



Zweikanaliges Sicherheitssystem

Hinsichtlich der grundlegenden Architektur der voranstehenden Abbildung sind auch einige weitere Aspekte zu berücksichtigen. Zunächst stellt sich die Frage, wie viele „Kanäle“ das System hat. Ein einkanaliges System würde bei Ausfall eines seiner Subsysteme ausfallen. Bei einem zweikanaligen (auch redundanten) System fällt erst nach zwei Fehlern – jeweils in einem der beiden Kanäle – das System aus. Dank der Zweikanaligkeit ist es gegenüber einer einzelnen Störung fehlertolerant und würde weiter funktionieren. Im Bild oben ist ein zweikanaliges System dargestellt.

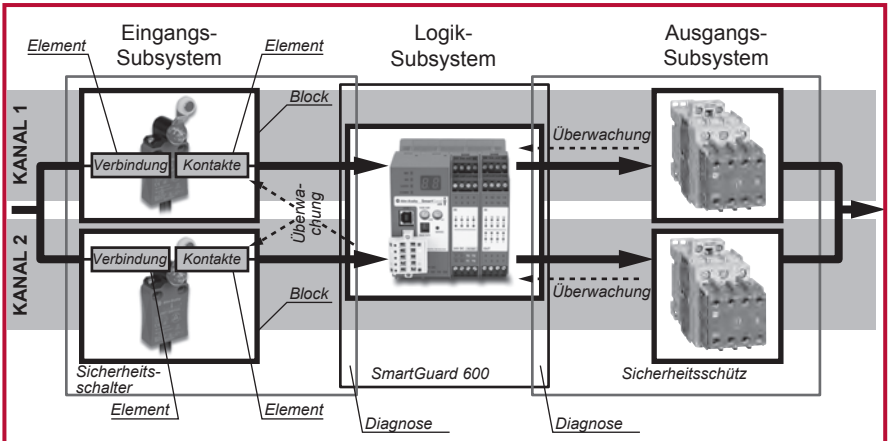
Ein zweikanaliges System ist im Fall eines gefährlichen Zustands eindeutig besser vor Ausfall geschützt als ein einkanaliges System. Die Zuverlässigkeit (in Bezug auf die Sicherheitsfunktion des Systems) kann jedoch noch weiter erhöht werden, wenn auch Diagnosemaßnahmen für die Fehlererkennung eingeschlossen werden. Nach Erkennung eines Fehlers muss natürlich eine entsprechende Reaktion erfolgen und das System in einen sicheren Zustand überführt werden. Die folgende Abbildung zeigt die Einbeziehung von Diagnosemaßnahmen mithilfe von Überwachungsverfahren.



Diagnose mit einem zweikanaligen Sicherheitssystem

In der Regel (aber nicht immer) verfügt das System in allen Subsystemen über je zwei Kanäle. In diesem Fall hat damit jedes Subsystem zwei Kanäle. In der Norm werden diese als „Blöcke“ beschrieben. Ein zweikanaliges Subsystem besteht aus mindestens zwei Blöcken, ein einkanaliges Subsystem aus mindestens einem Block. Manche Systeme können auch eine Kombination aus zweikanaligen und einkanaligen Blöcken umfassen.

Für eine genauere Untersuchung des Systems ist es erforderlich, die Einzelteile der Blocks zu betrachten. Das Tool SISTEMA verwendet für diese Einzelteile den Begriff „Elemente“.



Unterteiltes System mit Diagnosen mit einem zweikanaligen Sicherheitssystem

Das Eingangs-Subsystem ist in der Abbildung bis auf die Elementebene unterteilt. Das Ausgangsschütz-Subsystem ist bis auf Blockebene unterteilt, das Logik-Subsystem ist gar nicht unterteilt. Die Überwachungsfunktion sowohl für die Sicherheitsschalter als auch die Schütze wird in der Logiksteuerung ausgeführt. Daher weisen die Ein- bzw. Ausgangs-Subsysteme eine kleine Überschneidung mit dem Logik-Subsystem auf.

Dieses Prinzip der Unterteilung von Systemen findet sich als Methodik in der Norm EN ISO 13849-1 ebenso wie im grundlegenden Systemstruktur-Prinzip des SISTEMA-Tools. Es gibt jedoch einige feine Unterschiede, die unbedingt zu beachten sind. Die Norm ist methodisch nicht restriktiv. Für das vereinfachte Verfahren zur Bewertung des PL besteht der erste Schritt in der Regel darin, die Systemstruktur in Kanäle und jeden Kanal in Blocks aufzuteilen. Mit SISTEMA wird das System in der Regel zunächst in Subsysteme unterteilt. Die Norm enthält keine explizite Beschreibung eines Subsystem-Konzepts; die Verwendung eines solchen Konzepts gemäß SISTEMA ermöglicht jedoch eine verständlichere, intuitive Herangehensweise. Selbstverständlich ergeben sich daraus keine Auswirkungen auf die endgültige Berechnung: Im Tool SISTEMA und in der Norm werden jeweils dieselben Prinzipien und Formeln verwendet. Ferner soll darauf hingewiesen werden, dass das Subsystem-Konzept auch in der Norm EN/IEC 62061 verwendet wird.

Das oben verwendete Beispielsystem entspricht einem der fünf Systemarchitekturen, die in der Norm genannt werden. Anwender, die mit den Steuerungskategorien vertraut sind, werden bemerken, dass unser Beispiel ein Vertreter der Steuerungskategorie 3 oder 4 ist.

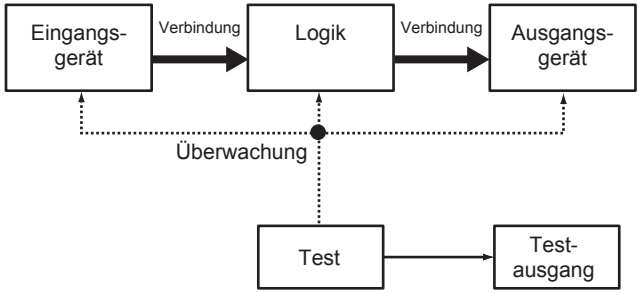
Die fünf Grundtypen der vorgesehenen Systemarchitekturen, die in der Norm verwendet werden, entsprechen den ursprünglichen Steuerungskategorien gemäß der alten Norm EN 954-1. In der neuen Norm werden diese als vorgesehene Architektur-Kategorien (Designated Architecture Categories) bezeichnet. Die Anforderungen für die Steuerungskategorien sind fast (jedoch nicht vollständig) mit den Anforderungen gemäß EN 954-1 identisch. Die vorgesehenen Architekturen sind in den folgenden Abbildungen dargestellt. Zu beachten ist, dass sie sowohl auf vollständige Systeme als auch auf Subsysteme angewendet werden können. Die Diagramme sind nicht als physikalische Struktur zu verstehen, sondern vielmehr als grafische Darstellung konzeptueller Anforderungen.

Vorgesehene Architektur für Steuerungskategorie B

Die vorgesehene Architektur für Steuerungskategorie B muss grundlegende Sicherheitsprinzipien (siehe Anhang der Norm EN ISO 13849-2) verwenden. Ein einzelner Fehler kann zu einem Ausfall des Systems bzw. Subsystems führen. Die vollständigen Anforderungen finden Sie in EN ISO 13849-1.

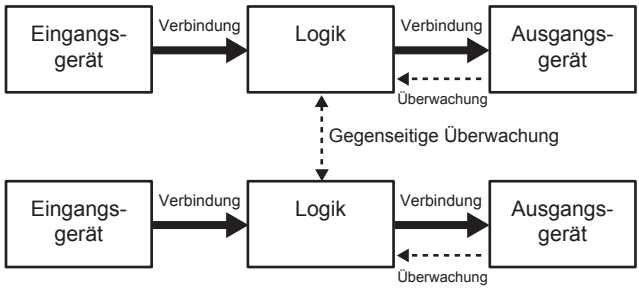
Vorgesehene Architektur für Steuerungskategorie 1

Die vorgesehene Architektur für Steuerungskategorie 1 hat dieselbe Struktur wie die Kategorie B. Auch bei der Kategorie 1 kann ein einzelner Fehler zu einem Ausfall führen. Da hier jedoch erprobte Sicherheitsprinzipien erforderlich sind (siehe Anhang der Norm EN ISO 13849-2) ist die Ausfallwahrscheinlichkeit geringer als bei der Kategorie B. Die vollständigen Anforderungen finden Sie in EN ISO 13849-1.



Vorgesehene Architektur für Steuerungskategorie 2

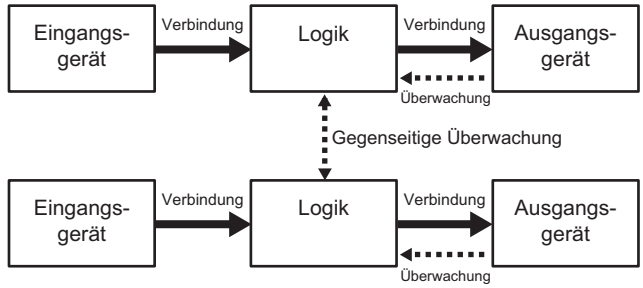
Die vorgesehene Architektur für Kategorie 2 muss grundlegende Sicherheitsprinzipien (siehe Anhang der Norm EN ISO 13849-2) verwenden. Über einen Funktionstest des Systems bzw. Subsystems wird zudem eine Diagnoseüberwachung vorhanden sein. Der Funktionstest muss bei der Inbetriebnahme sowie anschließend in regelmäßigen Abständen durchgeführt werden. Die Testhäufigkeit muss so hoch sein, dass einer Anfrage der Sicherheitsfunktion mindestens 100 Tests entsprechen. Auch bei der Kategorie 2 kann ein einzelner Fehler zu einem Ausfall des Systems bzw. Subsystems führen, die Ausfallwahrscheinlichkeit ist jedoch geringer als bei der Kategorie 1. Die vollständigen Anforderungen finden Sie in EN ISO -1.



Vorgesehene Architektur für Steuerungskategorie 3

Die vorgesehene Architektur für Kategorie 3 muss grundlegende Sicherheitsprinzipien (siehe Anhang der Norm EN ISO 13849-2) verwenden. Eine weitere Anforderung sieht einen Ausfall des Systems bzw. Subsystems bei einem einzelnen Fehler vor. Im Hinblick auf die Sicherheitsfunktion muss das System bzw. Subsystem also über eine einfache Fehlertoleranz verfügen. In der Regel wird zur Erfüllung dieser Anforderung eine zweikanalige Architektur wie in der Abbildung oben verwendet. Eine zusätzliche Anforderung ist die Erkennung des einzelnen Fehlers, soweit dies praktikabel ist. Diese Anforderung ist identisch mit der ursprünglichen Anforderung für die Kategorie 3 gemäß EN 954-1. In diesem Zusammenhang hat sich die

Bedeutung der Formulierung „soweit praktikabel“ als problematisch herausgestellt: Gemeint ist, dass die Kategorie 3 alle Arten von System – von einem System mit Redundanz, aber ohne Fehlererkennung (oft beschreibend, daher passend als „dumme Redundanz“ [„stupid redundancy“] bezeichnet) bis zu einem redundanten System mit Erkennung aller einzelnen Fehler – abdeckt. Um dieses Problem zu beheben, wurde in EN ISO 13849-1 die Anforderung zur Bewertung des Diagnosedeckungsgrads (DC) aufgenommen. Es lässt sich zeigen, dass bei steigender Zuverlässigkeit (MTTFd) des Systems ein niedrigerer DC erforderlich ist. Unabhängig davon sollten Architekturen der Kategorie 3 jedoch in jedem Fall einen DC von mindestens 60 % aufweisen.



Vorgesehene Architektur für Steuerungskategorie 4

Die vorgesehene Architektur für Kategorie 4 muss grundlegende Sicherheitsprinzipien (siehe Anhang der Norm EN ISO 13849-2) verwenden. Das Anforderungsdiagramm ist ähnlich wie bei der Kategorie 3, jedoch erfordert die Kategorie 4 stärkere Überwachung, d. h. einen höheren Diagnosedeckungsgrad. Grafisch dargestellt ist dies durch die fetteren Punktlinien, die zur Darstellung der Überwachungsfunktionen verwendet werden. Der wesentliche Unterschied zwischen den Kategorien 3 und 4 besteht darin, dass bei der Kategorie 3 die meisten Fehler erkannt werden müssen, bei Kategorie 4 dagegen alle Fehler. Der DC muss mindestens 99 % betragen. Selbst eine Kombination verschiedener Fehler darf nicht zu einem gefährlichen Ausfall führen.

Zuverlässigkeitsdaten

Im Rahmen der PL-Berechnung für die sicherheitsbezogenen Teile eines Steuerungssystems verwendet die Norm EN ISO 13849-1 quantitative Zuverlässigkeitsdaten. Dies stellt eine bedeutende Abweichung von der Norm EN ISO 954-1 dar. Daraus ergibt sich zunächst die Frage: „Woher können die entsprechenden Daten bezogen werden?“ Die Norm erlaubt zwar auch die Verwendung von Daten aus anerkannten Zuverlässigkeitshandbüchern, stellt gleichzeitig aber deutlich heraus, dass Daten vom Hersteller zu bevorzugen sind. Daher stellt Rockwell Automation die relevanten Informationen in Form einer Datenbibliothek für SISTEMA zur Verfügung. In einem ersten Schritt soll zunächst untersucht werden, welche Daten erforderlich sind und wie diese erzeugt werden.

Der wichtigsten Daten, die im Rahmen der PL-Berechnung gemäß der Norm (und gemäß SISTEMA) erforderlich sind, ist der PFH-Wert (probability of dangerous failure per hour – Wahrscheinlichkeit gefährlicher Ausfälle pro Stunde). Diese Daten entsprechen den PFHd-Daten gemäß EN/IEC 62061.

PL (Performance Level)	PFHd (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)	SIL (Safety Integrity Level)
a	$\geq 10^{-5}$ bis $<10^{-4}$	Keine
b	$\geq 3 \times 10^{-6}$ bis $<10^{-5}$	1
c	$\geq 10^{-6}$ bis $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ bis $<10^{-6}$	2
e	$\geq 10^{-8}$ bis $<10^{-7}$	3

Die Tabelle oben zeigt die Beziehung zwischen PFH, PL und SIL (Safety Integrity Level – Sicherheits-Integritätslevel). Für bestimmte Subsysteme wird der PFH gegebenenfalls vom Hersteller zur Verfügung gestellt, um die Berechnung zu erleichtern. Um die PFH-Daten bereitstellen zu können, muss ein Hersteller in der Regel relativ komplexe Berechnungen und/oder Tests an seinen Subsystemen vornehmen. Für den Fall, dass die PFH-Daten nicht zur Verfügung stehen, bietet die Norm EN ISO 1384913849-1 ein alternatives vereinfachtes Verfahren auf Grundlage des MTTFd („mean time to a dangerous failure“ – mittlere Zeit bis zu einem gefährlichen Ausfall) eines einzelnen Kanals. Anschließend kann der PL (und damit auch der PFH) eines Systems bzw. Subsystems mithilfe der Methoden und Formeln in der Norm berechnet werden. Mit SISTEMA ist die Berechnung noch einfacher und bequemer.

Hinweis: Es ist unbedingt zu beachten, dass für ein zweikanaliges System (mit oder ohne Diagnose) nicht 1/PFHd zum Bestimmen der MTTFd verwendet werden darf, wie von EN ISO 13849-1 gefordert. Diese Norm setzt die MTTFd eines einzelnen Kanals voraus. Dies ist ein ganz anderer Wert als die MTTFd der Kombination beider Kanäle eines zweikanaligen Subsystems. Wenn die Wahrscheinlichkeit gefährlicher Ausfälle pro Stunde (PFHd) eines zweikanaligen Subsystems bekannt ist, kann sie ganz einfach direkt in SISTEMA eingegeben werden.

MTTFd eines einzelnen Kanals

Dabei handelt es sich um die durchschnittliche mittlere Zeit bis zum Auftreten eines gefährlichen Fehlers, der zu einem Ausfall der Sicherheitsfunktion führen kann. Diese Zeit ist in Jahren ausgedrückt. Der MTTFd ist ein Durchschnittswert aus den MTTFd-Werten der jeweiligen „Blöcke“ der einzelnen Kanäle. Er kann sowohl auf Systeme als auch auf Subsysteme angewendet werden. Die Norm enthält die unten angegebene Formel zur Berechnung des Durchschnitts aus allen MTTFd-Werten der einzelnen Elemente, die in einem einkanaligen Kanal oder Subsystem verwendet werden.

In dieser Phase wird der Nutzen von SISTEMA deutlich. Zeitaufwändiges Nachschlagen in Tabellen und die Berechnung von Formeln werden überflüssig, da diese Aufgaben von der Software übernommen werden. Das Ergebnis der Berechnungen mit SISTEMA kann in Form eines mehrseitigen Berichts ausgedruckt werden.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$ (Formel D1 aus EN ISO 13849-1)

Bei den meisten zweikanaligen Systemen sind beide Kanäle identisch und das Ergebnis der Formel gilt entsprechend für jeden der beiden Kanäle.

Für Systeme bzw. Subsysteme, deren Kanäle nicht identisch sind, bietet die Norm eine spezielle Formel:

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Diese Formel ermittelt den Durchschnitt aus den beiden unterschiedlichen Kanälen. Zum Zwecke der Vereinfachung ist es zulässig, ausschließlich mit dem Wert des schlechteren Kanals zu arbeiten.

In der Norm wird der MTTFd in die drei folgenden Bereiche eingeteilt:

Bezeichnung des MTTFd für jeden Kanal	**Bereich des MTTFd für jeden Kanal**
Niedrig	3 Jahre <= MTTFd <10 Jahre
Mittel	10 Jahre <= MTTFd <30 Jahre
Hoch	30 Jahre <= MTTFd <100 Jahre

Stufen des MTTFd

Beachten Sie, dass EN ISO 13849-1 die nutzbare MTTFd eines einzelnen Kanals eines Subsystems auf maximal 100 Jahre beschränkt, auch wenn die tatsächlich abgeleiteten Werte wesentlich höher sein sollten.

Wie später gezeigt wird, wird anschließend auf Grundlage des erzielten MTTFd-Durchschnittsbereichs, der vorgesehenen Architektur (Kategorie) und des Diagnosedeckungsgrads (DC) eine vorläufige PL-Einstufung berechnet. Wir verwenden hier den Begriff „vorläufig“, da gegebenenfalls noch weitere Anforderungen erfüllt werden müssen, darunter die Systemintegrität sowie Maßnahmen zum Schutz vor Ausfall aufgrund gemeinsamer Ursache (Common Cause Failure).

Verfahren zur Kenngrößenbestimmung

Im Folgenden wird die Frage, wie ein Hersteller die Daten in Form des PFHd oder des MTTFd bestimmt, genauer untersucht. Das Verständnis dieser Zusammenhänge ist bei der Arbeit mit Herstellerdaten von wesentlicher Bedeutung. Komponenten können in drei Grundtypen unterteilt werden:

- mechanische Komponenten (elektro-mechanisch, mechanisch, pneumatisch, hydraulisch usw.)
- elektronische Komponenten
- Software-Komponenten

Zwischen den gemeinsamen Ausfallmechanismen dieser drei Technologiearten bestehen grundlegende Unterschiede. Diese werden im Folgenden zusammengefasst:

Mechanische Technologie:

Die Ausfallrate ist proportional zur inhärenten Zuverlässigkeit sowie zur Verwendungsrate. Je höher die Anwendung bzw. der Gebrauch, desto wahrscheinlicher die Störung oder der Ausfall eines der Einzelteile. Es wird darauf hingewiesen, dass dies nicht die einzige Ausfallursache ist; solange die Betriebszeit/-zyklen nicht eingegrenzt werden, ist es jedoch die wichtigste Ausfallursache. Es ist offensichtlich, dass Schütze mit einem Schaltzyklus von einmal in 10 Sekunden während einer kürzeren Dauer zuverlässig betrieben werden können als identische Schütze, die einmal täglich betrieben werden. Die Komponenten physikalischer Geräte werden in der Regel speziell für ihre spezifische Verwendung konzipiert. Die Komponenten werden geformt, gegossen, bearbeitet usw. Sie werden mit Verbindungselementen, Federn, Magneten, elektrischen Wicklungen usw. kombiniert, um einen Mechanismus zu bilden. Da für die Einzelteile in der Regel kein Verwendungsverlauf in anderen Anwendungen vorliegt, sind für diese Teile keine bestehenden Zuverlässigkeitsdaten verfügbar. Die Bewertung des PFHd oder des MTTFd für die Maschine erfolgt in der Regel auf Testbasis. Beide Normen EN/IEC 62061 und EN ISO 13849-1 empfehlen als Testverfahren das sogenannte B10d.

Bei der B10d-Prüfung wird eine bestimmte Anzahl Mustergeräte (in der Regel mindestens zehn) unter angemessen repräsentativen Bedingungen getestet. Die mittlere Anzahl Schaltspiele, die erreicht wird, bevor 10 % der Mustergeräte ausfallen und einen gefährlichen Zustand herstellen, wird B10d-Wert genannt. In der Praxis kommt es häufig vor, dass alle Mustergeräte beim Ausfall in einen sicheren Zustand überführt werden; für diesen Fall ist in der Norm jedoch festgelegt, dass als B10d-Wert (gefährlich) das Doppelte des B10-Werts (sicher) angenommen werden kann.

Elektronische Technologie:

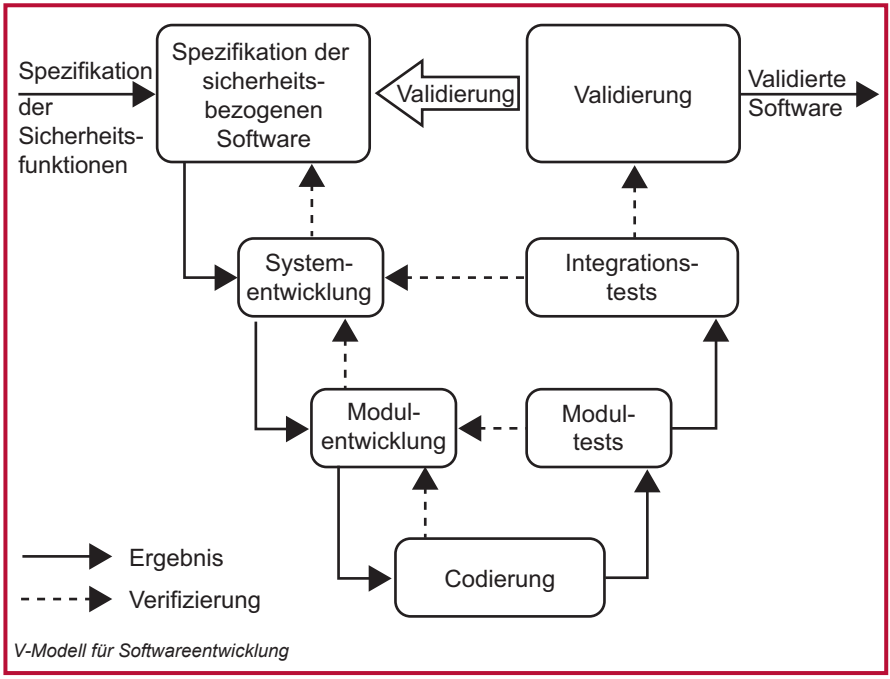
Es gibt keine beweglichen Teile, die materiellem Verschleiß ausgesetzt werden können. In einer Betriebsumgebung, die den spezifizierten elektrischen Leistungsmerkmalen, Temperaturleistungsmerkmalen usw. entspricht, ist der überwiegende Ausfall einer elektronischen Schaltung proportional zur inhärenten Zuverlässigkeit ihrer Komponenten (bzw. der fehlenden Zuverlässigkeit). Der Ausfall einzelner Komponenten kann viele verschiedene Ursachen haben. Fehler bei der Herstellung, übermäßige Strom-Transienten, mechanische Verbindungsprobleme usw. Im Allgemeinen können Ausfälle elektronischer Komponenten nur schwer durch Analysen vorhergesehen werden und sie scheinen willkürlich aufzutreten. Tests, die unter Testlaborbedingungen an einem elektronischen Gerät durchgeführt werden, ermöglichen es daher nicht unbedingt, typische langfristige Ausfallmuster zu erkennen.

Die Bestimmung der Zuverlässigkeit elektronischer Geräte erfolgt daher üblicherweise mithilfe von Analysen und Berechnungen. Geeignete Daten für die einzelnen Komponenten können aus Handbüchern mit Zuverlässigkeitsdaten entnommen werden. Über Analysen kann bestimmt werden, welche Komponenten-Ausfallarten gefährlich sind. Es ist sowohl zulässig als auch üblich, bei den Komponenten-Ausfallarten einen Durchschnitt von 50 % sicher und 50 % gefährlich anzunehmen. Damit werden in der Regel relativ konservative Daten gewonnen.

Die Norm IEC 61508 enthält Formeln zur Berechnung der Gesamtwahrscheinlichkeit gefährlicher Ausfälle (PFH oder PFD) des Geräts, d. h. Subsystems. Diese recht komplexen Formeln berücksichtigen (wo zutreffend) die Zuverlässigkeit der Komponenten, das Potenzial für einen Ausfall aufgrund gemeinsamer Ursache (CCF – Betafaktor), den Diagnosedeckungsgrad (DC), das Funktionstestintervall und das Prüftestintervall. Diese komplexen Berechnungen werden in der Regel vom Gerätehersteller durchgeführt. Sowohl nach EN/IEC 62061 als auch nach EN ISO 13849-1 ist ein auf diese Weise gemäß IEC 61508 berechnetes Subsystem zulässig. Der PFHd aus diesen Berechnungen kann direkt im Anhang K der EN ISO 13849-1 bzw. im Berechnungstool SISTEMA verwendet werden.

Software:

Software-Ausfälle sind inhärent systembedingt: Die Ursache eines Ausfalls hängt stets damit zusammen, wie das System entworfen, geschrieben oder kompiliert wurde. Daher werden alle Ausfälle von dem System verursacht, unter dem sie erzeugt werden, und nicht durch die Verwendung dieses Systems. Zur Kontrolle von Ausfällen muss daher das System kontrolliert werden. Beide Normen EN/IEC 61508 und EN ISO 13849-1 enthalten hierfür Anforderungen und Methoden. Dabei verwenden sie das klassische V-Modell. Im Einzelnen sollen die Anforderungen und Methoden an dieser Stelle nicht weiter vertieft werden.Embedded Software betrifft den Entwickler des Geräts. In der Regel wird Embedded Software im Einklang mit den in Teil 3 der Norm IEC 61508 dargestellten Verfahren entwickelt. Im Hinblick auf die Anwendersoftware enthalten die meisten programmierbaren Sicherungen „zertifizierte" Funktionsblöcke oder Routinen. Dadurch wird die Validierung der Anwendersoftware erleichtert. Es wird jedoch darauf hingewiesen, dass das fertiggestellte Anwendungsprogramm anschließend noch validiert werden muss. Es muss nachgewiesen werden, dass die Verknüpfung und Parametrierung der Blöcke ordnungsgemäß und für die beabsichtigte Aufgabe gültig sind. Beide Normen EN ISO 13849-1 und EN/IEC 62061 enthalten Leitlinien für diesen Prozess.



V-Modell für Softwareentwicklung

Diagnosedeckungsgrad

Dieses Thema wurde bereits im Zusammenhang mit den vorgesehenen Architekturen für die Steuerungskategorien 2, 3 und 4 angesprochen: Bei diesen Kategorien muss mithilfe von Diagnosetests geprüft werden, ob die Sicherheitsfunktion noch ordnungsgemäß funktioniert. Der Begriff „Diagnosedeckungsgrad“ (in der Regel abgekürzt als DC) dient zur Angabe, wie effizient diese Tests sind. Es is wichtig, zu beachten, dass der DC nicht allein auf der Anzahl der Komponenten basiert, bei denen ein gefährlicher Ausfall möglich ist, sondern die gesamte gefährliche Ausfallrate berücksichtigt. Das Symbol λ steht für die „Ausfallrate“. Der DC drückt das Verhältnis der jeweiligen Häufigkeit des Vorkommens der beiden folgenden gefährlichen Ausfalltypen aus:

Erkannter gefährlicher Ausfall („dangerous detected failure“, λd): Ausfälle, die zu einem Verlust der Sicherheitsfunktion führen könnten, die jedoch erkannt werden. Nach der Erkennung wird das Gerät mithilfe einer Fehlerreaktionsfunktion in einen sicheren Zustand überführt.

Gefährlicher Ausfall („dangerous failure“, λ): Alle Ausfälle, die potenziell zum Verlust der Sicherheitsfunktion führen können. Hierunter fallen sowohl erkannte als auch nicht erkannte Ausfälle. Wirklich gefährlich sind natürlich die nicht erkannten Ausfälle (λdu).

Der DC wird durch folgende Formel ausgedrückt:

DC = λdd/λd, ausgedrückt als Prozentsatz.

Der Begriff DC hat in EN ISO 13849-1 und EN/IEC 62061 dieselbe Bedeutung, die Ableitung des DC erfolgt in den beiden Normen jedoch auf unterschiedliche Weise. EN/IEC 62061 schlägt die Berechnung auf Grundlage einer Ausfallanalyse vor, EN ISO 13849-1 dagegen beschreibt ein vereinfachtes Verfahren mithilfe von Nachschlagetabellen: Verschiedene übliche Diagnoseverfahren werden zusammen mit dem zugehörigen erwarteten DC-Prozentsatz aufgeführt. In bestimmten Fällen sind dennoch rationale Entscheidungen erforderlich: Bei einigen Verfahren ist der erreichte DC-Prozentsatz zum Beispiel proportional zur Anzahl der Testdurchführungen. Es wird gelegentlich eingewandt, dass diese Methode zu ungenau sei. Die Schätzung des DC hängt unter Umständen jedoch von zahlreichen verschiedenen Variablen ab; unabhängig davon, welches Verfahren angewandt wird, kann das Ergebnis immer nur als Näherungswert verstanden werden.

Es soll außerdem darauf hingewiesen werden, dass die Tabellen in der Norm EN ISO 13849-1 auf umfangreichen Forschungsarbeiten des BGIA beruhen. Untersucht wurden die Ergebnisse mithilfe von tatsächlichen Diagnoseverfahren, die in echten Anwendungen verwendet werden. Im Sinne der Vereinfachung wird der DC in dieser Norm in vier Grundbereiche unterteilt:

<60 % = kein

60 % bis <90 % = niedrig

90 % bis <99 % = mittel

≥99 % = hoch

Diese Herangehensweise, bei der mit Bereichen statt mit einzelnen Prozentwerten gearbeitet wird, ist im Hinblick auf die Genauigkeit, die erzielt werden kann, realistischer. Das Tool SISTEMA verwendet die in der Norm beschriebenen Nachschlagetabellen. Mit der steigenden Komplexität der Elektronik in Sicherheitsgeräten nimmt auch die Wichtigkeit des DC zu. Es ist davon auszugehen, dass bei zukünftigen Bearbeitungen der Normen der Klärung dieser Fragestellung noch größeres Gewicht zukommt. Bis dahin sollte es ausreichend sein, den geeigneten DC-Bereich auf Grundlage der Erfahrung im Engineering-Bereich und vernünftiger Überlegungen auszuwählen.

Ausfälle mit gemeinsamer Ursache

In den meisten zweikanaligen Systemen bzw. Subsystemen (d. h. solchen mit einfacher Fehlertoleranz) beruht das Diagnoseprinzip auf der Voraussetzung, dass nicht bei beiden Kanälen gleichzeitig ein gefährlicher Ausfall auftritt. Statt „gleichzeitig“ wäre es genauer zu sagen „innerhalb des Diagnose-Testintervalls“. Bei einem angemessen kurzen Diagnose-Testintervall (z. B. unter acht Stunden) kann sinnvoll angenommen werden, dass die Wahrscheinlichkeit für das Auftreten zweier getrennter unabhängiger Fehler innerhalb dieser Zeit sehr gering ist. Die Norm weist jedoch ausdrücklich darauf hin, dass die Frage, ob die Fehlermöglichkeiten wirklich voneinander getrennt und unabhängig sind, genau untersucht werden muss. Kann zum Beispiel eine Störung in einer Komponente vorhersehbar zum Ausfall anderer Komponenten führen, wird die Gesamtmenge der daraus resultierenden Störungen als ein einzelner Ausfall erachtet.

Es ist ferner möglich, dass ein Ereignis, das zu einem Ausfall einer Komponente führt, auch zum Ausfall weiterer Komponenten führt. Dieser Fall wird als „Ausfall aufgrund gemeinsamer Ursache“ bezeichnet (Common Cause Failure), gewöhnlich als CCF abgekürzt. Die CCF-Neigung wird gewöhnlich als Betafaktor (ß-Faktor) beschrieben. Entwickler von Subsystemen und von Systemen müssen die möglichen CCF unbedingt berücksichtigen. Es gibt verschie-

dene CCF-Typen und entsprechend verschiedene Möglichkeiten zu ihrer Vermeidung. Die Norm EN ISO 13849-1 schlägt einen vernünftigen Mittelweg zwischen zu großer Komplexität und zu starker Vereinfachung ein. Wie die Norm EN/IEC 62061 verfolgt sie eine überwiegend qualitative Methode. Sie enthält eine Aufstellung der Maßnahmen, deren Wirksamkeit bei der Vermeidung von CCF bekannt ist.

Anzahl	Messung im Vergleich zu CCF	Punktzahl
1	Separation/Segregation	15
2	Diversität	20
3	Entwicklung/Anwendung/Erfahrung	20
4	Beurteilung/Analyse	5
5	Kompetenz/Schulung	5
6	Schutzart	35

Bewertung für Ausfälle aufgrund gemeinsamer Ursache

Bei der Entwicklung eines Systems bzw. Subsystems muss eine ausreichende Menge dieser Maßnahmen implementiert sein. Zwar lässt sich durchaus berechtigt einwenden, dass die ausschließliche Verwendung dieser Liste zur Vermeidung aller möglichen CCF nicht ausreicht. Betrachtet man die Absicht dieser Liste genauer, wird jedoch klar: Zweck dieser Anforderung ist es, dass Entwickler die möglichen CCF analysieren und auf Grundlage der Art der Technologie und der Leistungsmerkmale der geplanten Anwendung geeignete Maßnahmen zu ihrer Vermeidung implementieren. Durch die Verwendung der Liste wird die Berücksichtigung einiger der grundlegendsten und wirkungsvollsten Verfahren gestärkt, darunter die Vielfalt der verschiedenen Ausfallarten und Leistungsvorgaben bei der Entwicklung. Auch das BGIA-Tool SISTEMA erfordert die Implementierung der CCF-Nachschlagetabellen aus der Norm und macht diese Tabellen bequem verfügbar.

Systematische Fehler

In diesem Dokument wurden sicherheitsrelevante Zuverlässigkeitsdaten bereits in Form von MTTFd und der Wahrscheinlichkeit gefährlicher Ausfälle erörtert. Dies ist jedoch nicht ausreichend. Bei Verwendung dieser Begriffe wurde die Annahme zugrunde gelegt, dass die Ausfälle in ihrem Wesen zufällig zu sein scheinen. In der Norm IEC/EN 62061 wird für die Wahrscheinlichkeit für zufällige Hardware-Ausfälle speziell die Abkürzung PFHd verwendet. Es gibt jedoch ferner auch einige Ausfalltypen, die der Gruppe der „systembedingten Ausfälle“ angehören. Diese sind auf Fehler beim Entwicklungs- oder Fertigungsprozess zurückzuführen. Typisches Beispiel dafür sind Fehler im Software-Code. Anhang G der Norm enthält Maßnahmen zur Vermeidung solcher Fehler (und damit der Ausfälle). Zu diesen Maßnahmen gehören die Verwendung der geeigneten Materialien und Fertigungsverfahren, Prüfungen, Analysen und Computersimulation. Ausfälle können ferner durch vorhersehbare Ereignisse und Besonderheiten ausgelöst werden, die in der Betriebsumgebung auftreten können, sofern die Auswirkungen dieser Ereignisse nicht gesteuert werden. Auch hierfür stehen in Anhang G Maßnahmen bereit. Ein Beispiel für ein vorhersehbares Ereignis ist ein gelegentlicher Abbruch der Stromversorgung. Daher muss das System bei Abschaltung von Komponenten in einen sicheren Zustand überführt werden. Diese Maßnahmen können durchaus schlicht als gesunder Menschenverstand betrachtet werden. Als Grundlage zur Gewährleistung der Sicherheit sind sie jedoch unverzichtbar: Werden die Steuerung und Vermeidung systembedingter Ausfälle nicht angemessen berücksichtigt, sind alle übrigen Anforderungen der Normen gegenstandslos. Gegebenenfalls können dadurch auch dieselben Arten von Maßnahmen erforderlich sein, die bei der Steuerung zufälliger Hardware-Ausfälle (zur Erzielung des erforderlichen PFHd) verwendet werden, wie automatische Diagnosetests und redundante Hardware.

Fehlerausschluss

Eines der primären Analysetools für Sicherheitssysteme ist die Analyse von Ausfällen. Entwickler und Anwender müssen verstehen, wie das Sicherheitssystem bei Fehlern reagiert. Für diese Analyse stehen zahlreiche Techniken zur Verfügung. Zu den Beispielen gehören die Fehlerbaumanalyse, Fehlermodi, Auswirkungen, die Analyse kritischer Zustände, die Ereignisbaumanalyse sowie Belastungsprüfungen.

Während der Analyse können bestimmte Fehler unentdeckt bleiben, da diese nicht mit automatischen Diagnosetests erkannt werden können, ohne unangemessene wirtschaftliche Kosten zu verursachen. Außerdem ist die Wahrscheinlichkeit, dass diese Fehler auftreten, eventuell verschwindend gering, wenn entsprechende Entwicklungs-, Konstruktions- und Testmethoden verwendet werden. Unter diesen Bedingungen brauchen die Fehler nicht mehr berücksichtigt werden. Beim Fehlerausschluss wird das Auftreten eines Fehlers ausgeschlossen, da die Wahrscheinlichkeit, dass dieser spezielle Fehler im sicherheitsbezogenen Steuerungssystem auftritt, vernachlässigbar ist.

ISO 13849-1:2006 ermöglicht den Fehlerausschluss basierend auf der technischen Unwahrscheinlichkeit des Auftretens, der allgemein anerkannten technischen Erfahrung und der technischen Anforderungen, die sich auf die Anwendung beziehen. ISO 13849-2:2003 stellt Beispiele und Rechtfertigungen zum Ausschließen bestimmter Fehler für elektrische, pneumatische, hydraulische und mechanische Systeme zur Verfügung. Fehlerausschlüsse müssen mit einer detaillierten Rechtfertigung in der technischen Dokumentation angegeben werden.

Es ist nicht immer möglich, sicherheitsbezogene Steuerungssysteme zu beurteilen, ohne davon auszugehen, dass bestimmte Fehler ausgeschlossen werden können. Ausführliche Informationen zu Fehlerausschlüssen finden Sie in der Norm ISO 13849-2.

Je höher das Risiko ist, desto strenger muss die Rechtfertigung von Fehlerausschlüssen sein. Wenn PLe für die Implementierung einer Sicherheitsfunktion durch ein sicherheitsbezogenes Steuerungssystem erforderlich ist, darf man sich im Allgemeinen nicht allein auf Fehlerausschlüsse verlassen, um diesen Performance Level zu erreichen. Dies hängt von der verwendeten Technologie und der vorgesehenen Betriebsumgebung ab. Daher ist es wichtig, dass der Entwickler bei der Verwendung von Fehlerausschlüssen umso vorsichtiger vorgeht, je höher diese PL-Anforderung ist.

Beispielsweise muss ein Türzuhaltungssystem, das PLe erzielen muss, über eine minimale Fehlertoleranz von 1 (z. B. zwei konventionelle mechanische Positionsschalter) verfügen, um diesen Performance Level zu erreichen, da normalerweise der Ausschluss von Fehlern wie gebrochene Schalterbetätiger nicht zu rechtfertigen ist. Es ist jedoch eventuell akzeptabel, Fehler auszuschließen, wie z. B. einen Verdrahtungskurzschluss innerhalb eines Schaltschranks, der in Übereinstimmung mit relevanten Industrienormen entwickelt wurde.

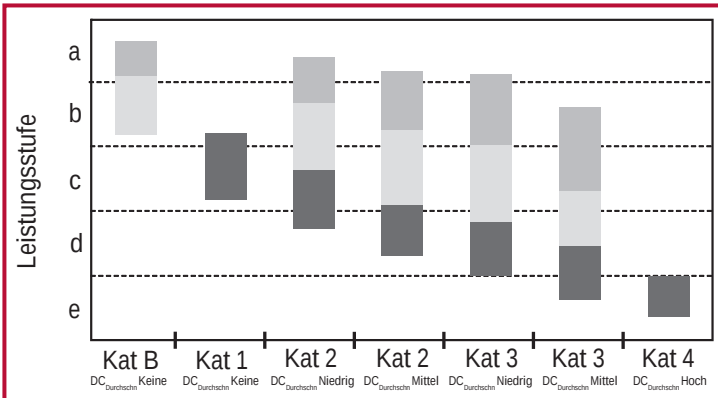
Performance Level (PL)

Beim Performance Level handelt es sich um eine diskrete Stufe, die die Fähigkeit der sicherheitsbezogenen Teile des Steuerungssystems angibt, eine Sicherheitsfunktion auszuführen.

Um den PL zu beurteilen, der durch die Realisierung einer der fünf definierten Architekturen erzielt wurde, müssen für das System (oder Subsystem) folgende Daten vorhanden sein:

- MTTFd (mittlerer Abstand zwischen gefährlichen Ausfällen der einzelnen Kanäle)
- DC (Diagnoseabdeckung)
- Architektur (die Kategorie)

Das folgende Diagramm zeigt eine grafische Methode zum Bestimmen des Performance Levels aus der Kombination dieser Faktoren. Die Tabelle am Ende dieses Dokuments zeigt die tabellarischen Ergebnisse verschiedener Markov-Modelle, die als Grundlage für dieses Diagramm dienen. Eine ausführlichere Bestimmung kann anhand dieser Tabelle vorgenommen werden.



Grafische Bestimmung des Performance Levels (PL)

Andere Faktoren müssen ebenfalls berücksichtigt werden, um den erforderlichen Performance Level zu erreichen. Zu diesen Anforderungen gehören die Vorkehrungen für Ausfälle aufgrund gemeinsamer Ursache, systembedingte Ausfälle, Umgebungsbedingungen und Einsatzzeit.

Wenn die Wahrscheinlichkeit eines gefährlichen Ausfalls (PFHd) des Systems oder Subsystems bekannt ist, kann Tabelle 10.4 (Anhang K der Norm) zum Ableiten des Performance Levels (PL) verwendet werden.

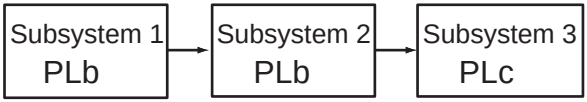
Aufbau und Kombinationen des Subsystems

Subsysteme, die einem Performance Level entsprechen, können einfach anhand Tabelle 10.3 zu einem System kombiniert werden. Die Bedeutung dieser Tabelle ist eindeutig: Erstens kann das System nur so gut sein wie sein schwächstes Subsystem. Zweitens gilt, je mehr Subsysteme vorliegen, desto größer die Möglichkeit eines Ausfalls.

$PL_{niedrig}$	$N_{niedrig}$	PL
a	>3	unzulässig
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Die Berechnung des Performance Levels für in Reihe kombinierte Subsysteme

In dem im folgenden Diagramm dargestellten System weisen die Subsysteme 1 und 2 den niedrigsten Performance Level (jeweils PLb) auf. Daher kann anhand der Tabelle in der Zeile b (in der Spalte $PL_{niedrig}$) bis 2 (in der Spalte $N_{niedrig}$) festgestellt werden, dass der erzielte Performance Level des Systems „b“ lautet (in der Spalte PL). Wenn alle drei Subsysteme den Performance Level PLb aufweisen, wäre die erzielte PL PLa.



Kombination einer Reihe von Subsystemen zu einem PLb-System

Validierung

Die Validierung spielt bei der Entwicklung und Inbetriebnahme von Sicherheitssystemen eine wichtige Rolle. In ISO/EN 13849-2:2003 sind die Validierungsanforderungen festgelegt. Sie erfordert einen Validierungsplan und erörtert die Validierung durch Test- und Analysetechniken wie z. B. die Fehlerbaumanalyse und Fehlermodi, Auswirkungen und die Analyse kritischer Zustände. Die meisten dieser Anforderungen beziehen sich auf den Hersteller des Subsystems und nicht auf den Anwender des Subsystems.

Inbetriebnahme der Maschine

Während der Inbetriebnahme eines Systems oder einer Maschine müssen die Sicherheitsfunktionen in allen Betriebsarten validiert werden. Diese Validierung muss alle normalen und vorhersehbaren anormalen Bedingungen abdecken. Kombinationen der Eingänge und Betriebsabfolgen sind ebenfalls zu berücksichtigen. Dieses Verfahren ist deshalb so wichtig, da stets überprüft werden muss, dass das System für die tatsächlichen Betriebs- und Umgebungsbedingungen geeignet ist. Einige dieser Merkmale unterscheiden sich eventuell von denen, die bei der Entwicklung erwartet werden.

Systemaufbau gemäß IEC/EN 62061

IEC/EN 62061, „Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“. Hierbei handelt es sich um die maschinenspezifische Realisierung der Norm IEC/EN 61508. Diese Norm definiert die Anforderungen für die Entwicklung der Systemebene aller sicherheitsbezogenen elektrischen Steuerungssysteme in Maschinen sowie für die Entwicklung nicht komplexer Subsysteme oder Geräte.

Die Risikobeurteilung führt zu einer Risikominderungsstrategie, die wiederum den Bedarf an sicherheitsbezogenen Steuerungsfunktionen definiert. Diese Funktionen müssen dokumentiert werden und Folgendes umfassen:

- Eine Spezifikation der funktionalen Anforderungen
- Eine Spezifikation der Anforderungen an die Sicherheitsintegrität

Zu den funktionalen Anforderungen zählen Details wie Betriebshäufigkeit, erforderliche Reaktionszeit, Betriebsarten, Arbeitszyklen, Betriebsumgebung und Fehlerreaktionsfunktionen. Die Anforderungen an die Sicherheitsintegrität werden in sogenannten Sicherheits-Integritätslevels (SILs) ausgedrückt. Abhängig von der Komplexität des Systems müssen einige oder alle Elemente in der folgenden Tabelle berücksichtigt werden, um zu bestimmen, ob der Systemaufbau die Anforderungen der erforderlichen SIL erfüllt.

Element, das für den SIL berücksichtigt werden muss	**Symbol**
Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde	PFHd
Hardwarefehlertoleranz	Kein Symbol
Anteil ungefährlicher Ausfälle	SFF
Prüfintervall	T_1
Diagnosetestintervall	T_2
Anfälligkeit für Ausfälle aufgrund gemeinsamer Ursache	ß
Diagnoseabdeckung	DC

Elemente für SIL

Subsysteme

Der Begriff „Subsystem“ hat in der Norm IEC/EN 62061 eine besondere Bedeutung. Es handelt sich um die erste Unterteilung eines Systems in Teile, die bei ihrem Ausfall zu einem Ausfall der Sicherheitsfunktion führen würden. Wenn daher zwei redundante Schalter in einem System verwendet werden, ist keiner der beiden Einzelschalter ein Subsystem. Das Subsystem würde aus beiden Schaltern und der zugehörigen Fehlerdiagnosefunktion (sofern vorhanden) bestehen.

Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFHd)

IEC/EN 62061 verwendet dieselben grundlegenden Methoden, die auch im Abschnitt zur Norm EN ISO 13849-1 erläutert wurden, um Ausfallraten auf Komponentenebene zu bestimmen. Dieselben Bestimmungen und Methoden gelten auch für „mechanistische“ und elektronische Komponenten. In der Norm IEC/EN 62061 wird die MTTFd in Jahren nicht berücksichtigt. Die Ausfallrate pro Stunde (λ) wird entweder direkt berechnet, abgerufen oder vom B10-Wert anhand der folgenden Formel abgeleitet:

λ = 0,1 x C/B10 (dabei gilt: C = Anzahl der Betriebszyklen pro Stunde)

Die Normen unterscheiden sich erheblich, was die Methode zum Bestimmen der Gesamt-PFHd für ein Subsystem oder System angeht. Es muss eine Analyse der Komponenten vorgenommen werden, um die Wahrscheinlichkeit eines Ausfalls der Subsysteme bestimmen zu können. Es stehen vereinfachte Formeln für die Berechnung gängiger Subsystemarchitekturen zur Verfügung (diese sind weiter hinten im Text beschrieben. Wenn diese Formeln nicht geeignet sind, müssen komplexere Berechnungsmethoden wie z. B. Markov-Modelle eingesetzt werden. Die Wahrscheinlichkeit eines gefährlichen Ausfalls (PFHd) der einzelnen Subsysteme wird anschließend addiert, um die Gesamt-PFHd für das System zu bestimmen. Anschließend kann anhand von Tabelle 15 (Tabelle 3 der Norm) bestimmt werden, welcher Sicherheits-Integritätslevel (SIL) für diesen Bereich der PFHd angemessen ist.

$$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$$

Die Formeln für diese Architektur berücksichtigen die parallele Anordnung der Subsystemelemente und fügen die beiden folgenden Elemente aus der vorherigen Tabelle hinzu.

ß (Beta) ist die Anfälligkeit für Fehler aufgrund gemeinsamer Ursache

SIL (Safety Integrity Level)	**PFHd (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)**
3	$\geq 10^{-8}$ bis $<10^{-7}$
2	$\geq 10^{-7}$ bis $<10^{-6}$
1	$\geq 10^{-6}$ bis $<10^{-5}$

Wahrscheinlichkeit eines gefährlichen Ausfalls für SILs

Die PFHd-Daten für ein Subsystem werden normalerweise vom Hersteller bereitgestellt. Die Daten für Rockwell Automation-Sicherheitskomponenten und -Systeme stehen auf unterschiedliche Weise zur Verfügung, unter anderem auf folgender Webseitee:

www.discoverrockwellautomation.com/safety

IEC/EN 62061 macht außerdem deutlich, dass ggf. auch Handbücher zu Zuverlässigkeitsdaten verwendet werden können.

Bei elektromechanischen Geräten mit geringer Komplexität wird der Ausfallmechanismus mit der Anzahl und Häufigkeit der Vorgänge und nicht nur mit der Zeit verknüpft. Daher werden für diese Komponenten die Daten aus einer Art Test abgeleitet (z. B. dem B10-Test, der im Kapitel zu EN ISO 13849-1 beschrieben ist). Anwendungsbasierte Daten, wie z. B. die erwartete Anzahl der Vorgänge pro Jahr, sind erforderlich, um B10d oder ähnliche Daten in PFHd umzuwandeln.

Hinweis: Im Allgemeinen gilt Folgendes (bei Berücksichtigung eines Faktors zum Ändern der Jahre in Stunden):

PFHd = 1/MTTFd

Es ist jedoch unbedingt zu beachten, dass für ein zweikanaliges System (mit oder ohne Diagnose) nicht 1/PFHd zum Bestimmen der MTTFd verwendet werden darf, wie von EN ISO 13849-1 gefordert. Diese Norm setzt die MTTFd eines einzelnen Kanals voraus. Dies ist ein ganz anderer Wert als die MTTFd der Kombination beider Kanäle eines zweikanaligen Subsystems.

Architektonische Einschränkungen

Das grundlegende Merkmal von IEC/EN 62061 ist, dass das Sicherheitssystem in Subsysteme unterteilt ist. Der SIL-Wert der Hardware, der für ein Subsystem festgelegt werden kann, ist nicht nur durch die Wahrscheinlichkeit eines gefährlichen Ausfalls (PFHd), sondern auch durch die Hardwarefehlertoleranz und den Anteil ungefährlicher Ausfälle des Subsystems begrenzt. Unter Hardwarefehlertoleranz versteht man die Fähigkeit eines Systems, seine Funktion auch beim Vorliegen von Fehlern auszuführen. Eine Fehlertoleranz von null bedeutet, dass die Funktion nicht ausgeführt wird, sobald ein einziger Fehler auftritt. Eine Fehlertoleranz von eins bedeutet, dass das Subsystem seine Funktion auch dann ausführt, wenn ein einziger Fehler vorliegt. Der Anteil ungefährlicher Ausfälle entspricht dem Teil der Gesamtausfallrate, der nicht zu einem gefährlichen Ausfall führt. Die Kombination dieser beiden Elemente gilt als architektonische Einschränkung und wird als SIL Claim Limit (SIL CL) bezeichnet. Die folgende Tabelle zeigt die Beziehung zwischen architektonischer Einschränkung und SILCL. Ein Subsystem (und daher sein System) muss die PFHd-Anforderungen und die architektonischen Einschränkungen sowie weitere relevante Bestimmungen der Norm erfüllen.

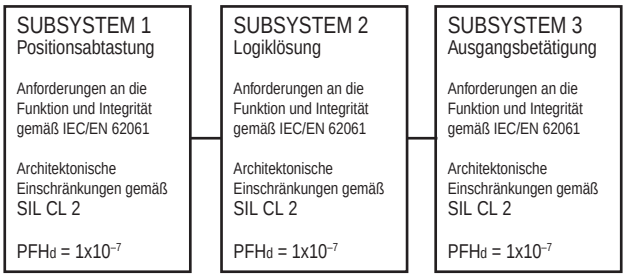
Anteil ungefährlicher Ausfälle	Hardwarefehlertoleranz		
	0	1	2
<60 %	Nur zulässig, wenn bestimmte Ausnahmen gelten	SIL1	SIL2
60 %–<90 %	SIL1	SIL2	SIL3
90 %–<99 %	SIL2	SIL3	SIL3
≥99 %	SIL3	SIL3	SIL3

Architektonische Einschränkungen des SIL

Beispielsweise ist die Architektur eines Subsystems, das über eine Ein-Fehler-Toleranz verfügt und einen Anteil ungefährlicher Ausfälle von 75 % aufweist, auf eine Klassifizierung von maximal SIL2 beschränkt, ganz gleich, wie hoch die Wahrscheinlichkeit gefährlicher Ausfälle ist. Bei der Kombination von Subsystemen wird der durch das sicherheitsbezogene Steuerungssystem erreichte SIL so eingeschränkt, dass er kleiner oder gleich der niedrigsten SIL-Anspruchsgrenze (SIL CL) eines beliebigen Subsystems ist, das einen Teil der sicherheitsbezogenen Steuerungsfunktion darstellt.

Systemrealisierung

Um die Wahrscheinlichkeit gefährlicher Ausfälle zu berechnen, ist jede Sicherheitsfunktion in Funktionsblöcke zu unterteilen, die anschließend als Subsysteme erkannt werden. Die Implementierung eines Systemaufbaus für eine typische Sicherheitsfunktion würde ein Sensorgerät umfassen, das an einem mit einem Aktor verbundenen Logikgerät angeschlossen ist. So entsteht eine Reihenanordnung von Subsystemen. Wie bereits dargelegt, gilt Folgendes: Wenn die Wahrscheinlichkeit eines gefährlichen Ausfalls für jedes Subsystem bestimmt werden kann und dessen SIL CL bekannt ist, lässt sich die Ausfallwahrscheinlichkeit des Systems problemlos durch Addieren der Ausfallwahrscheinlichkeit der Subsysteme berechnen. Dieses Konzept wird im Folgenden verdeutlicht.


SUBSYSTEM 1
Positionsabtastung
Anforderungen an die Funktion und Integrität gemäß IEC/EN 62061
Architektonische Einschränkungen gemäß SIL CL 2
PFHd = 1x10-7
SUBSYSTEM 2
Logiklösung
Anforderungen an die Funktion und Integrität gemäß IEC/EN 62061
Architektonische Einschränkungen gemäß SIL CL 2
PFHd = 1x10-7
SUBSYSTEM 3
Ausgangsbetätigung
Anforderungen an die Funktion und Integrität gemäß IEC/EN 62061
Architektonische Einschränkungen gemäß SIL CL 2
PFHd = 1x10-7

= PFH_d [1] + PFH_d [2] + PFH_d [3]
= $1x10^{-7}$ + $1x10^{-7}$ + $1x10^{-7}$
= $3x10^{-7}$, d. h. für SIL2 geeignet

Wenn beispielsweise SIL2 erreicht werden soll, muss jedes Subsystem ein SIL Claim Limit (SIL CL) von mindestens SIL2 aufweisen. Die Summe der Wahrscheinlichkeit eines gefährlichen Ausfalls (PFHd) für das System darf den Grenzwert nicht überschreiten, der in der vorherigen Tabelle als Wahrscheinlichkeit gefährlicher Ausfälle für SILs aufgeführt ist.

Aufbau des Subsystems – IEC/EN 62061

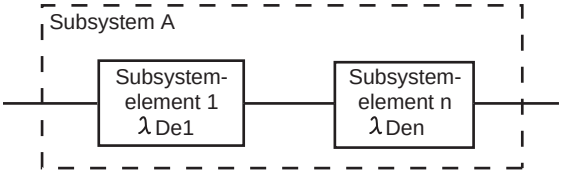
Wenn ein Systementwickler Komponenten verwendet, die gemäß IEC/EN 62061 sofort in Subsysteme integriert werden können, kann er sich dadurch die Arbeit wesentlich erleichtern, da die speziellen Anforderungen an den Aufbau des Subsystems nicht anzuwenden sind. Diese Anforderungen werden in der Regel vom Hersteller des Geräts (Subsystems) abgedeckt und sind wesentlich komplexer als die für die Entwicklung der Systemebene.

IEC/EN 62061 erfordert, dass komplexe Subsysteme, wie z. B. Sicherheits-SPS, mit IEC 61508 oder anderen entsprechenden Normen übereinstimmen. Dies bedeutet, dass für Geräte, die komplexe elektronische oder programmierbare Komponenten verwenden, die volle Härte der Norm IEC 61508 greift. Dies kann sehr schwierig und aufwändig sein. Beispielsweise ist die Beurteilung der PFHd eines komplexen Subsystems ein äußerst komplizierter Vorgang, bei dem Techniken wie die Erstellung von Markov-Modellen, Zuverlässigkeits-Blockdiagramme oder Fehlerbaumanalysen zum Einsatz kommen.

IEC/EN 62061 nennt keine Anforderungen für die Entwicklung weniger komplexer Subsysteme. In der Regel würde dies relativ einfache elektrische Komponenten wie Verriegelungsschalter und elektromechanische Sicherheitsrelais umfassen. Die Anforderungen sind nicht so komplex wie die in IEC 61508, können aber dennoch relativ kompliziert sein.

IEC/EN 62061 definiert vier Logikarchitekturen für Subsysteme. Darüber hinaus werden Formeln zur Verfügung gestellt, mit denen die PFHd berechnet werden kann, die durch ein Subsystem mit geringer Komplexität erzielt wird. Diese Architekturen sind rein logische Darstellungen und dürfen nicht als physische Architekturen betrachtet werden. Die vier Logikarchitekturen für Subsysteme mit den entsprechenden Formeln werden in den vier folgenden Diagrammen veranschaulicht.

Für eine grundlegende Subsystemarchitektur, wie sie im Folgenden dargestellt ist, werden die Wahrscheinlichkeiten eines gefährlichen Ausfalls einfach addiert.

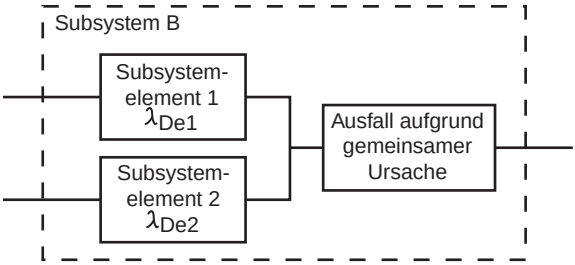


Logikarchitektur A für Subsysteme

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$
$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, Lambda stellt die Ausfallrate dar. Die Einheiten der Ausfallrate sind Ausfälle pro Stunde. λ_D entspricht der Rate gefährlicher Ausfälle. λ_{DssA} entspricht der Rate gefährlicher Ausfälle des Subsystems A. Lambda DssA ist die Summe der Ausfallraten der einzelnen Elemente e1, e2, e3 bis einschließlich en. Die Wahrscheinlichkeit eines gefährlichen Ausfalls wird mit 1 Stunde multipliziert, um die Wahrscheinlichkeit eines Ausfalls innerhalb einer Stunde zu berechnen.

Das nächste Diagramm zeigt ein System mit Ein-Fehler-Toleranz ohne Diagnosefunktion. Wenn die Architektur eine Ein-Fehler-Toleranz umfasst, besteht die Möglichkeit eines Ausfalls aufgrund gemeinsamer Ursache, welche daher berücksichtigt werden muss. Die Ableitung des Ausfalls aufgrund gemeinsamer Ursache wird weiter hinten in diesem Kapitel kurz beschrieben.



Logikarchitektur B für Subsysteme

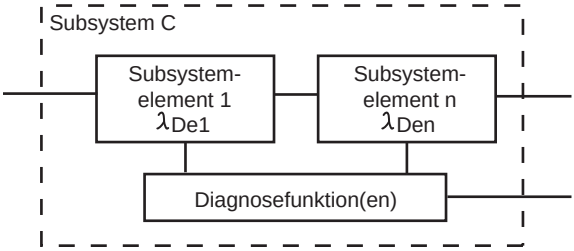
$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$
$PFH_{DssB} = \lambda_{DssB} \times 1h$

Die Formeln für diese Architektur berücksichtigen die parallele Anordnung der Subsystemelemente und fügen die beiden folgenden Elemente aus der vorherigen Tabelle „Elemente für SIL“ hinzu.

ß – Die Anfälligkeit für Fehler aufgrund gemeinsamer Ursache (Beta)

T1 – Das Prüfintervall oder die Betriebszeit, je nachdem, welcher Wert kleiner ist. Bei der Beständigkeitsprüfung sollen Fehler und Verschlechterungen des Sicherheitssubsystems erkannt werden, damit der Betriebszustand des Subsystems wiederhergestellt werden kann. In der Praxis entspricht dies einem Austausch (genau wie der äquivalente Begriff „Einsatzzeit“ (Mission Time) in der Norm EN ISO 13849-1).

Das nächste Diagramm zeigt die funktionale Darstellung eines Systems mit einer Null-Fehler-Toleranz und Diagnosefunktion. Die Diagnoseabdeckung soll die Wahrscheinlichkeit gefährlicher Hardwareausfälle senken. Die Diagnosetests werden automatisch ausgeführt. Die Definition von Diagnosedeckungsgrad entspricht der in der Norm EN ISO 13849-1, also das Verhältnis der Rate erkannter gefährlicher Ausfälle im Vergleich zur Rate aller gefährlichen Ausfälle.

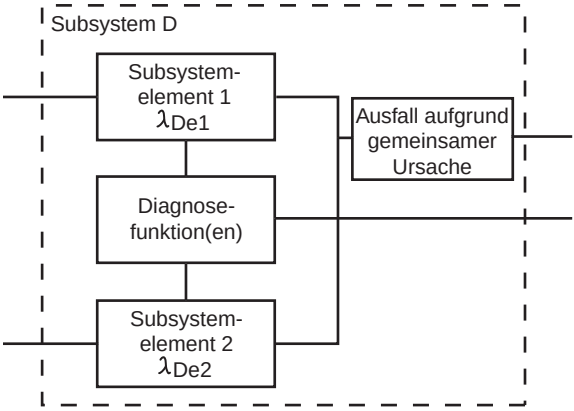


Logikarchitektur C für Subsysteme

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$
$PFH_{DssC} = \lambda_{DssC} \times 1h$

Diese Formeln umfassen die Diagnoseabdeckung (Diagnostic Coverage; DC) für jedes Subsystemelement. Die Ausfallraten aller Subsysteme werden durch die Diagnoseabdeckung aller Subsysteme verringert.

Im vierten Beispiel ist die Architektur eines Subsystems abgebildet. Dieses Subsystem verfügt über eine Ein-Fehler-Toleranz und umfasst eine Diagnosefunktion. Bei Systemen mit Ein-Fehler-Toleranz muss auch die Möglichkeit eines Ausfalls aufgrund gemeinsamer Ursache berücksichtigt werden.



Logikarchitektur D für Subsysteme

Falls die Subsystemelemente unterschiedlich sind, wird die folgende Formel verwendet:

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

Falls die Subsystemelemente identisch sind, wird die folgende Formel verwendet:

$\lambda_{DssD} = (1 - ß)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1-DC)] \times T_1 \} + ß \times \lambda_{De}$
$PFH_{DssD} = \lambda_{DssD} \times 1h$

Beachten Sie, dass beide Formeln nur einen zusätzlichen Parameter verwenden: das Diagnoseintervall T2. Dies ist lediglich eine regelmäßige Überprüfung der Funktion. Dieser Test ist weniger umfassend als die Beständigkeitsprüfung.

Angenommen, die folgenden Werte werden für das Beispiel verwendet, in dem die Subsystemelemente unterschiedlich sind:

ß = 0,05
$\lambda_{De} = 1 \times 10^{-6}$ Ausfälle/Stunde
T1 = 87 600 Stunden (10 Jahre)
T2 = 2 Stunden
DC = 90 %

PFH_{DssD} = 5.791E-08 gefährliche Ausfälle pro Stunde. Dies läge innerhalb des für SIL3 erforderlichen Bereichs.

Auswirkungen des Prüfintervalls

IEC/EN 62061 gibt an, dass ein Prüfintervall von 20 Jahren bevorzugt wird (jedoch nicht obligatorisch ist). Nun werden die Auswirkungen näher betrachtet, die das Prüfintervall auf das System hat. Wenn die Formel mit T1 = 20 Jahre erneut berechnet wird, ergibt sich Folgendes: PFHDssD = 6.581E-08. Dies liegt noch immer innerhalb des für SIL3 erforderlichen Bereichs. Der Entwickler muss stets daran denken, dass dieses Subsystem mit anderen Subsystemen kombiniert werden muss, damit die Gesamtrate der gefährlichen Ausfälle berechnet werden kann.

Auswirkungen der Analyse von Ausfällen aufgrund gemeinsamer Ursache

Nun werden die Auswirkungen näher betrachtet, die die Ausfälle aufgrund gemeinsamer Ursache auf das System haben. Angenommen, es werden zusätzliche Maßnahmen ergriffen und der Betawert (ß) verbessert sich auf 1 % (0,01), während das Prüfintervall unverändert bei 20 Jahren bleibt. Die Rate gefährlicher Ausfälle verbessert sich auf 2.71E-08, was bedeutet, dass das Subsystem nun besser für den Einsatz in einem SIL3-System geeignet ist.

Ausfälle aufgrund gemeinsamer Ursache

Unter Ausfällen aufgrund gemeinsamer Ursache versteht man mehrere Ausfälle aufgrund einer einzigen Ursache, die zu einem gefährlichen Ausfall führen. Informationen zu Ausfällen aufgrund gemeinsamer Ursache sind in der Regel nur für den Entwickler des Subsystems, also den Hersteller, erforderlich. Sie sind Teil der Formel, die zum Abschätzen der Wahrscheinlichkeit eines gefährlichen Ausfalls für ein Subsystem angegeben wurde. Sie werden normalerweise nicht auf Systementwicklungsebene benötigt.

In Anhang F der Norm IEC/EN 62061 ist ein einfaches Konzept für die Abschätzung der Ausfälle aufgrund gemeinsamer Ursache beschrieben. Die folgende Tabelle enthält eine Zusammenfassung des Bewertungsprozesses.

Anzahl	Messung im Vergleich zu CCF	Punktzahl
1	Separation/Segregation	25
2	Diversität	38
3	Entwicklung/Anwendung/Erfahrung	2
4	Beurteilung/Analyse	18
5	Kompetenz/Schulung	4
6	Schutzart	18

Bewertung der Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ursache

Es werden Punkte für das Ergreifen von Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ursache vergeben. Die Punktzahl wird addiert, um den Faktor für die Ausfälle aufgrund

gemeinsamer Ursache zu bestimmen (siehe die folgende Tabelle). Der Betafaktor wird in den Subsystemmodellen verwendet, um die Ausfallrate „anzupassen“.

Gesamtpunktzahl	Faktor für Ausfälle aufgrund gemeinsamer Ursache (ß)
<35	10 % (0,1)
35–65	5 % (0,05)
65–85	2 % (0,02)
85–100	1 % (0,01)

Betafaktor für Ausfälle aufgrund gemeinsamer Ursache

Diagnosedeckungsgrad (DC)

Mithilfe automatischer Diagnosetests soll die Wahrscheinlichkeit gefährlicher Hardwareausfälle verringert werden. Ideal wäre es, wenn alle gefährlichen Hardwareausfälle erkannt würden, doch in der Praxis liegt dieser Wert bei 99 % (dies kann auch durch 0,99 ausgedrückt werden).

Der Diagnosedeckungsgrad ist das Verhältnis der Wahrscheinlichkeit erkannter gefährlicher Ausfälle zur Wahrscheinlichkeit aller gefährlichen Ausfälle.

$$DC = \frac{\text{Wahrscheinlichkeit erkannter gefährlicher Ausfälle, } \lambda_{DD}}{\text{Wahrscheinlichkeit aller gefährlichen Ausfälle, } \lambda_{Dtotal}}$$

Der Wert der Diagnoseabdeckung liegt zwischen null und eins.

Hardwarefehlertoleranz

Die Hardwarefehlertoleranz stellt die Anzahl der Fehler dar, die ein Subsystem konstant halten kann, bevor es einen gefährlichen Ausfall verursacht. Beispielsweise bedeutet eine Hardwarefehlertoleranz von 1, dass zwei Fehler zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führen könnten, ein Fehler jedoch nicht.

Verwaltung der funktionalen Sicherheit

Die Norm definiert Anforderungen zur Kontrolle der Verwaltungs- und technischen Aktivitäten, die erforderlich sind, um ein sicherheitsbezogenes elektrisches Steuerungssystem zu erhalten.

Prüfintervall

Das Prüfintervall stellt die Zeit dar, nach der ein Subsystem entweder vollständig überprüft oder ersetzt werden muss, um sicherzustellen, dass es noch immer „wie neu“ ist. In der Praxis wird dies im Maschinensektor durch den Austausch von Subsystemen erzielt. Das Prüfintervall entspricht in der Regel der Betriebszeit. Die Norm EN ISO 13849-1:2008 verweist auf diese Zeit als Einsatzzeit (Mission Time).

Eine Beständigkeitsprüfung stellt eine Untersuchung dar, bei der Fehler und die Verschlechterung eines sicherheitsbezogenen Steuerungssystems erkannt werden können, damit das sicherheitsbezogene Steuerungssystem wieder in einen Zustand gebracht werden kann, der praktisch „wie neu“ ist. Die Beständigkeitsprüfung muss 100 % aller gefährlichen Ausfälle erkennen. Separate Kanäle müssen separat getestet werden.

Im Gegensatz zu den automatisch ausgeführten Diagnoseprüfungen werden die Beständigkeitsprüfungen in der Regel manuell und offline vorgenommen. Durch diese Automatik werden Diagnoseprüfungen häufig ausgeführt. Im Vergleich dazu sind Beständigkeitsprüfungen eher selten. Beispielsweise können die Schaltkreise, die zu einem Verriegelungsschalter an einer Schutztür führen, mit einer Diagnoseprüfung (z. B. einem Impulstest) automatisch auf Kurzschlüsse und Drahtbrüche getestet werden.

Das Prüfintervall muss vom Hersteller genannt werden. Manchmal gibt der Hersteller verschiedene Prüfintervalle an.

Anteil ungefährlicher Ausfälle

Der Anteil ungefährlicher Ausfälle entspricht in etwa der Diagnoseabdeckung, berücksichtigt jedoch auch alle inhärenten Tendenzen für einen Ausfall, bei dem ein sicherer Zustand aktiviert wird. Wenn beispielsweise eine Sicherung durchbrennt, kommt es zu einem Ausfall. Es ist jedoch sehr wahrscheinlich, dass der Ausfall zu einem Drahtbruch führt, was wiederum in den meisten Fällen ein „sicherer“ Ausfall ist. Der Anteil ungefährlicher Ausfälle SFF ist (die Summe der Rate „sicherer“ Ausfälle und der Rate der erkannten gefährlichen Ausfälle) dividiert durch (die Summe der Rate „sicherer“ Ausfälle und der Rate der erkannten und nicht erkannten gefährlichen Ausfälle). Es muss unbedingt erkannt werden, dass nur die Ausfalltypen berücksichtigt werden dürfen, die Auswirkungen auf die Sicherheitsfunktion haben könnten.

Die meisten mechanischen Geräte mit geringer Komplexität wie Not-Halt-Taster und Verriegelungsschalter weisen (selbst) einen Anteil ungefährlicher Ausfälle (SFF) auf. Die meisten elektronischen Sicherheitsgeräte wurden mit Redundanz- und Überwachungsfunktionen entwickelt, sodass bei diesen ein Anteil ungefährlicher Ausfälle von über 90 % gängig ist. Der Wert für den Anteil ungefährlicher Ausfälle wird normalerweise vom Hersteller angegeben.

Der Anteil ungefährlicher Ausfälle kann mit der folgenden Gleichung berechnet werden:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

Dabei gilt:

λ_S = Rate der sicheren Ausfälle

$\Sigma\lambda_S + \Sigma\lambda_D$ = Rate aller Ausfälle

λ_{DD} = Rate der erkannten gefährlichen Ausfälle

λ_D = Rate der gefährlichen Ausfälle.

Systembedingter Ausfall

Die Norm definiert Anforderungen für die Kontrolle und Vermeidung systembedingter Ausfälle. Systembedingte Ausfälle unterscheiden sich von zufälligen Hardwareausfällen, bei denen es sich um Ausfälle handelt, die zu einer willkürlichen Zeit auftreten und in der Regel ihre Ursache in einer Verschlechterung der Hardwareteile haben. Typische systembedingte Ausfälle, die auftreten können, sind Softwareentwicklungsfehler, Hardwarekonstruktionsfehler, falsche Spezifikationen der Anforderungen und Betriebsverfahren. Beispiele für die Schritte, die zum Vermeiden systembedingter Fehler erforderlich sind:

- Richtige Auswahl, Kombination, Anordnung, Montage und Installation von Komponenten
- Anwendung einer vernünftigen Engineeringpraxis
- Einhalten der Spezifikationen und der Installationsanleitung des Herstellers
- Sicherstellen der Kompatibilität zwischen den Komponenten
- Eignung für die Umgebungsbedingungen
- Verwendung geeigneter Materialien.

Überlegungen zur Struktur sicherheitsbezogener Steuerungssysteme

Überblick

In diesem Kapitel werden die allgemeinen Überlegungen und Prinzipien zur Struktur näher betrachtet, die beim Entwickeln eines sicherheitsbezogenen Steuerungssystems für eine beliebige Norm berücksichtigt werden müssen. Dabei bedient sich dieses Kapitel der Sprache der Kategorien aus der auslaufenden Norm EN 954-1, da die Kategorien primär die Struktur der Steuerungssysteme ansprechen.

Kategorien von Steuerungssystemen

Die „Kategorien" der Steuerungssysteme stammen aus der auslaufenden Norm EN 954-1:1996 (ISO 13849-1:1999). Allerdings werden sie häufig verwendet, um Sicherheitssteuerungssysteme zu beschreiben. Sie bleiben dabei ein integrierter Bestandteil der Norm EN ISO 13849-1 wie im Abschnitt zur Einführung in die funktionale Sicherheit von Steuerungssystemen beschrieben.

Es gibt fünf Kategorien, die die Fehlerreaktionsleistung eines sicherheitsbezogenen Steuerungssystems beschreiben. Eine Zusammenfassung dieser Kategorien finden Sie in Tabelle 19. Die folgenden Anmerkungen beziehen sich auf die Tabelle.

> **Anmerkung 1:** Kategorie B weist selbst keine besonderen Maßnahmen für die Sicherheit auf, bildet jedoch die Grundlage für die übrigen Kategorien.
>
> **Anmerkung 2:** Mehrfachfehler, die durch eine gemeinsame Ursache oder als unvermeidbare Folgen des ersten Fehlers entstanden sind, gelten als einzelne Fehler.
>
> **Anmerkung 3:** Die Fehleruntersuchung kann auf zwei kombinierte Fehler begrenzt werden (wenn sich dies rechtfertigen lässt), doch komplexe Schaltungen (z. B. Mikroprozessoren) erfordern möglicherweise mehr kombinierte Fehler.

Kategorie 1 zielt auf die Vermeidung von Fehlern ab. Erreicht wird dies durch geeignete Gestaltungsgrundsätze, Komponenten und Materialien. Einfachheit von Prinzip und Konstruktion in Verbindung mit gleichbleibenden und vorhersagbaren Materialeigenschaften sind die Schlüssel zu dieser Kategorie.

Die Kategorien 2, 3 und 4 fordern, dass Fehler erkannt (und geeignete Maßnahmen ergriffen) werden müssen, wenn Fehler nicht vermeidbar sind.

Redundanz, Diversität und Überwachung sind die Schlüssel zu diesen Kategorien. Unter Redundanz versteht man die Verdoppelung derselben Technik. Diversität besteht, wenn zwei verschiedene Techniken eingesetzt werden. Mit der Überwachung wird der Status der Geräte überprüft, wodurch anschließend die geeigneten Maßnahmen abhängig vom Status ergriffen werden kann. Das übliche (aber nicht das einzige) Überwachungsverfahren besteht darin, die sicherheitskritischen Funktionen zu verdoppeln und die Vorgänge zu vergleichen.

Zusammenfassung der Anforderungen	Systemverhalten
KATEGORIE B (siehe Anmerkung 1) Sicherheitsbezogene Teile von Maschinensteuerungen und/oder ihre Schutzeinrichtungen sowie ihre Komponenten müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, konstruiert, ausgewählt und zusammengestellt werden, dass sie den zu erwartenden Einflüssen standhalten können. Es sind die grundlegenden Sicherheitsprinzipien anzuwenden.	Wenn ein Fehler auftritt, kann es zum Ausfall der Sicherheitsfunktion kommen.
KATEGORIE 1 Es gelten die Anforderungen der Kategorie B in Verbindung mit dem Einsatz bewährter Sicherheitskomponenten und Sicherheitsprinzipien.	Wie für Kategorie B beschrieben, doch mit höherer sicherheitsgerichteter Zuverlässigkeit der sicherheitsgerichteten Funktion. (Je höher die Zuverlässigkeit, desto geringer die Wahrscheinlichkeit eines Fehlers.)
KATEGORIE 2 Es gelten die Anforderungen der Kategorie B und bewährte Sicherheitsprinzipien. Prüfung der Sicherheitsfunktion(en) bei Anlauf der Maschine und regelmäßige Prüfung durch die Maschinensteuerung. Wenn ein Fehler erkannt wird, muss ein sicherer Zustand aktiviert werden. Ist dies nicht möglich, muss eine Warnung erfolgen. EN ISO 13849-1 geht davon aus, dass die Testrate mindestens 100 Mal höher ist als die Anforderungsrate. EN ISO 13849-1 geht davon aus, dass die MTTFd der externen Testgeräte größer ist als die Hälfte der MTTFd der funktionalen Geräte, die getestet werden.	Der Ausfall der Sicherheitsfunktion wird durch die Prüfung erkannt. Das Auftreten eines Fehlers kann zum Ausfall der Sicherheitsfunktion zwischen Prüfintervallen führen.
KATEGORIE 3 (siehe Anmerkung 2 und 3) Es gelten die Anforderungen der Kategorie B und bewährte Sicherheitsprinzipien. Das System ist so zu gestalten, dass ein einzelner Fehler in einem Teil nicht zum Ausfall der Sicherheitsfunktion führt. Sofern praktikabel, muss ein einzelner Fehler erkannt werden.	Wenn der einzelne Fehler auftritt, wird die Sicherheitsfunktion immer ausgeführt. Es werden nicht alle Fehler erkannt. Eine Häufung unerkannter Fehler kann zum Ausfall der Sicherheitsfunktion führen.
KATEGORIE 4 (siehe Anmerkung 2 und 3) Es gelten die Anforderungen der Kategorie B und bewährte Sicherheitsprinzipien. Das System muss so aufgebaut sein, dass ein einzelner Fehler in einem Teil nicht zum Ausfall der Sicherheitsfunktion führt. Der einzelne Fehler wird erkannt, wenn oder bevor die nächste Anforderung der Sicherheitsfunktion erfolgt. Falls diese Erkennung nicht möglich ist, darf eine Fehlerhäufung nicht zum Ausfall der Sicherheitsfunktion führen.	Wenn die Fehler auftreten, wird die Sicherheitsfunktion immer ausgeführt. Die Fehler werden rechtzeitig erkannt, um einen Ausfall der Sicherheitsfunktionen zu vermeiden.

Kategorie B

Kategorie B stellt grundlegende Anforderungen an jedes Steuerungssystem, ganz gleich, ob es sicherheitsbezogen ist oder nicht. Ein Steuerungssystem muss in seiner vorgesehenen Umgebung arbeiten. Das Konzept der Zuverlässigkeit ist die Grundlage für Steuerungssysteme, da Zuverlässigkeit definiert ist als die Wahrscheinlichkeit, mit der ein Gerät seine vorgesehene Funktion für ein bestimmtes Intervall unter erwarteten Bedingungen ausführt.

Kategorie B erfordert die Anwendung grundlegender Sicherheitsprinzipien. ISO 13849-2 nennt die grundlegenden Sicherheitsprinzipien für elektrische, pneumatische, hydraulische und mechanische Systeme. Die Prinzipien für elektrische Systeme können wie folgt zusammengefasst werden:

- Richtige Auswahl, Kombination, Anordnung, Montage und Installation (d. h. gemäß den Anweisungen des Herstellers)
- Kompatibilität der Komponenten mit Spannungen und Strömen
- Eignung für die Umgebungsbedingungen
- Verwendung des Ausschaltprinzips
- Überspannungsschutz
- Verkürzung der Reaktionszeit
- Schutz vor unerwarteter Inbetriebnahme
- Sicheres Anbringen der Eingangsgeräte (z. B. Montage von Verriegelungen)
- Schutz des Steuerstromkreises (gemäß NFPA 79 & IEC 60204-1)
- Richtige Schutzverbindungen

Der Entwickler muss die richtigen Komponenten gemäß den Anweisungen des Herstellers auswählen, installieren und montieren. Diese Geräte müssen innerhalb der erwarteten Spannungs- und Strombereiche arbeiten. Die erwarteten Umgebungsbedingungen, wie elektromagnetische Verträglichkeit, Vibrationen, Stöße, Verunreinigungen und Spritzwasser, müssen ebenfalls berücksichtigt werden. Es wird das Ausschaltprinzip verwendet: Über den Schützspulen ist ein Überspannungsschutz installiert. Der Motor ist vor Überlasten geschützt. Verdrahtung und Erdung entsprechen den zutreffenden Elektronormen.

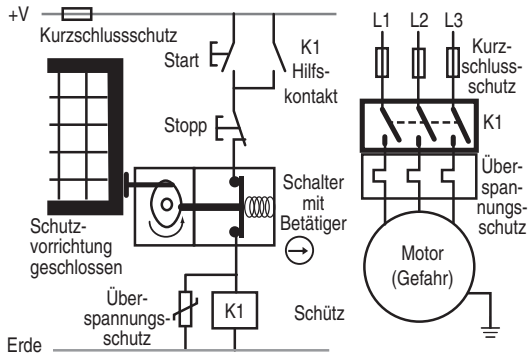
Kategorie 1

Kategorie 1 erfordert, dass das System die Bedingungen von Kategorie B erfüllt und dass bewährte Sicherheitskomponenten verwendet werden. Was genau sind Sicherheitskomponenten und woher weiß man, ob sie sich bewährt haben? ISO 13849-2 beantwortet solche Fragen für mechanische, hydraulische, pneumatische und elektrische Systeme. In Anhang D werden die elektrischen Komponenten näher beschrieben.

Komponenten gelten als „bewährt“, wenn sie erfolgreich in vielen ähnlichen Anwendungen eingesetzt wurden. Neu entwickelte Sicherheitskomponenten gelten als „bewährt“, wenn sie in Übereinstimmung mit den entsprechenden Normen entwickelt und verifiziert wurden.

Bewährte Komponente	**Norm**
Schalter mit positiver Betätigung (Direktöffnung)	IEC 60947-5-1
Not-Halt-Gerät	ISO 13850, IEC 60947-5-5
Sicherung	IEC 60269-1
Leistungsschalter	IEC 60947-2
Schütze	IEC 60947-4-1, IEC 60947-5-1
Mechanisch verbundene Kontakte	IEC 60947-5-1
Hilfsschütz (z. B. Schütz, Steuerungsrelais, positiv angesteuerte Relais)	EN 50205 IEC 60204-1, IEC 60947-5-1
Transformator	IEC 60742
Kabel	IEC 60204-1
Verriegelungen	ISO 14119
Temperaturschalter	IEC 60947-5-1
Druckschalter	IEC 60947-5-1 + pneumatische oder hydraulische Anforderungen
Steuer- und Schutzschaltgerät oder -anlage (CPS)	IEC 60947-6-2
Speicherprogrammierbare Logiksteuerung	IEC 61508, IEC 62061

Wenn im vorliegenden System der Kategorie B bewährte Komponenten eingesetzt werden, würde der Endschalter durch einen Direktöffnerschalter mit Betätiger ersetzt und das Schütz würde überdimensioniert werden, um einen besseren Schutz vor verschweißten Kontakten bieten zu können.



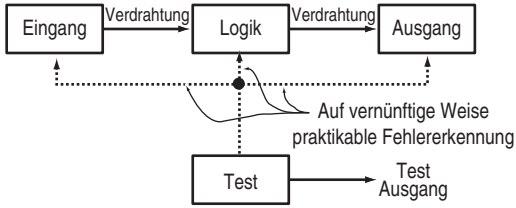
Einfaches Sicherheitssystem der Kategorie 1

Die Abbildung zeigt die Änderungen, die an einem einfachen System der Kategorie B vorgenommen werden müssen, um ein System der Kategorie 1 zu erhalten. Die Verriegelung und das Schütz spielen Schlüsselrollen bei der Unterbrechung der Energie zum Aktor, wenn Zugang zur Gefahrenquelle erforderlich ist. Der Sicherheitsschalter mit Betätiger erfüllt die Anforderungen der Norm IEC 60947-5-1 hinsichtlich der Direktöffnerkontakte. Dies wird durch das Pfeilsymbol im Kreis symbolisiert. Mit den bewährten Komponenten ist die Wahrscheinlichkeit, dass die Energiezufuhr unterbrochen wird, für Kategorie 1 höher als für Kategorie B. Die Verwendung bewährter Komponenten soll den Ausfall der Sicherheitsfunktion verhindern. Auch mit diesen Verbesserungen kann ein einziger Fehler weiterhin zum Ausfall der Sicherheitsfunktion führen.

Die Kategorien B und 1 basieren auf Prävention. Sie zielen darauf ab, eine gefährliche Situation zu vermeiden. Wenn Prävention alleine das Risiko nicht ausreichend senken kann, muss eine Fehlererkennung verwendet werden. Die Kategorien 2, 3 und 4 basieren auf Fehlererkennung, wobei für höhere Stufen der Risikominderung auch strengere Anforderungen gelten.

Kategorie 2

Für Kategorie 2 muss das System nicht nur die Anforderungen von Kategorie B erfüllen und bewährte Sicherheitsprinzipien verwenden, sondern muss auch Tests unterzogen werden. Die Tests müssen darauf ausgelegt sein, Fehler innerhalb der sicherheitsbezogenen Teile des Steuerungssystems zu erkennen. Falls keine Fehler erkannt werden, darf die Maschine ihre Funktion ausführen. Werden Fehler erkannt, muss der Test einen Befehl ausgeben. Sofern möglich, muss der Befehl die Maschine stets in einen sicheren Zustand bringen.



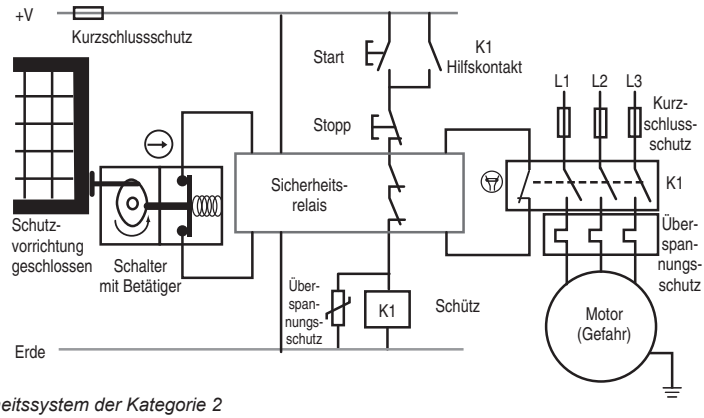
Der Test muss Fehler auf einigermaßen praktikable Weise erkennen können. Die Geräte, die den Test ausführen, können in das Sicherheitssystem integriert sein oder einen separaten Teil der Anlage darstellen.

Die Tests sind wie folgt auszuführen:

- beim ersten Einschalten der Maschine
- vor dem Initiieren einer Gefahr und
- regelmäßig, wenn es durch die Risikobeurteilung als notwendig erachtet wird.

Hinweis: EN ISO 138491-1 geht bei dem Test von einem Anforderungsverhältnis der Sicherheitsfunktion von 100:1 aus. Das hier angeführte Beispiel würde diese Anforderung nicht erfüllen.

Die Formulierungen „sofern möglich“ und „auf einigermaßen praktikable Weise“ deuten darauf hin, dass nicht alle Fehler erkennbar sind. Da es sich hierbei um ein einkanaliges System handelt (d. h. ein Draht überträgt Eingangsdaten an die Logik und an den Ausgang), kann ein einziger Fehler zum Ausfall der Sicherheitsfunktion führen. In einigen Fällen kann Kategorie 2 nicht vollständig auf ein Sicherheitssystem angewandt werden, da nicht alle Komponenten überprüft werden können.

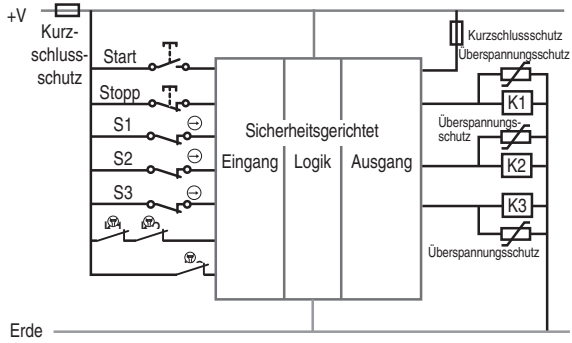


Sicherheitssystem der Kategorie 2

Die Abbildung hier zeigt ein einfaches System der Kategorie 1, das so verbessert wurde, dass es die Anforderungen von Kategorie 2 erfüllt. Die Tests werden von einem Sicherheitsrelais (MSR – Monitoring Safety Relay) ausgeführt. Beim Einschalten überprüft das Sicherheitsrelais die internen Komponenten. Werden keine Fehler erkannt, überprüft das Sicherheitsrelais den Schalter mit Betätiger, indem es die Ein-/Ausschaltvorgänge seiner Kontakte überwacht. Werden keine Fehler erkannt, und ist die Schutztür geschlossen, überprüft das Sicherheitsrelais das Ausgangsgerät: die mechanisch verbundenen Kontakte des Schützes. Werden keine Fehler erkannt, und ist das Schütz ausgeschaltet, aktiviert das Sicherheitsrelais seinen internen Ausgang und verbindet die Spule von K1 mit der Stopptaste. An diesem Punkt können die nicht sicherheitsbezogenen Teile des Steuerungssystems (also der Start-/Stopp-/Verriegelungsschaltkreis) die Maschine ein- und ausschalten.

Beim Öffnen der Schutztür werden die Ausgänge des Sicherheitsrelais deaktiviert. Beim erneuten Schließen der Schutztür wiederholt das Sicherheitsrelais die Tests für das Sicherheitssystem. Wenn keine Fehler erkannt werden, aktiviert das Sicherheitsrelais seinen internen Ausgang. Dank des Sicherheitsrelais erfüllt dieser Schaltkreis die Anforderungen für Kategorie 2, da das Eingangsgerät, das Logikgerät (also das Sicherheitsrelais selbst) und das Ausgangsgerät getestet werden. Der Test wird beim ersten Einschalten und vor dem Initiieren einer Gefahr ausgeführt.

Dank der inhärenten Logikfunktionen kann ein SPS-basiertes Sicherheitssystem so konzipiert sein, dass es die Anforderungen für Kategorie 2 erfüllt. Wie in der Erläuterung zu Kategorie 1 oben bereits erwähnt, wird die bewährte Anpassung der SPS (einschließlich ihrer Testfunktionen) zur wahren Herausforderung. Bei komplexen Sicherheitssystemen, die für Kategorie 2 klassifiziert werden müssen, muss anstelle der nicht sicherheitsbezogenen SPS eine sicherheitsbezogene SPS gemäß IEC 61508 verwendet werden.



Komplexes Sicherheitssystem der Kategorie 2

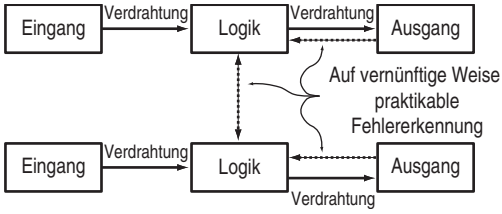
Dieses Beispiel zeigt ein komplexes System mit einer sicherheitsbezogenen SPS. Eine sicherheitsbezogene SPS erfüllt die Anforderung, dass es sich um ein bewährtes System handeln muss, da sie gemäß einer geeigneten Norm entwickelt wurde. Die mechanisch verbundenen Kontakte der Schütze werden zu Testzwecken am Eingang der SPS angeschlossen. Abhängig von der Programmierlogik können diese Kontakte an einer Eingangsklemme in Reihe geschaltet oder an einzelnen Eingangsklemmen angeschlossen werden.

Auch wenn bewährte Sicherheitskomponenten verwendet werden, kann ein einziger Fehler, der zwischen den Tests auftritt, zu einem Ausfall der Sicherheitsfunktion führen. Daher werden Systeme der Kategorie 2 in Anwendungen mit geringeren Risiken eingesetzt. Wenn höhere Fehlertoleranzen erforderlich sind, muss das Sicherheitssystem die Anforderungen von Kategorie 3 oder 4 erfüllen.

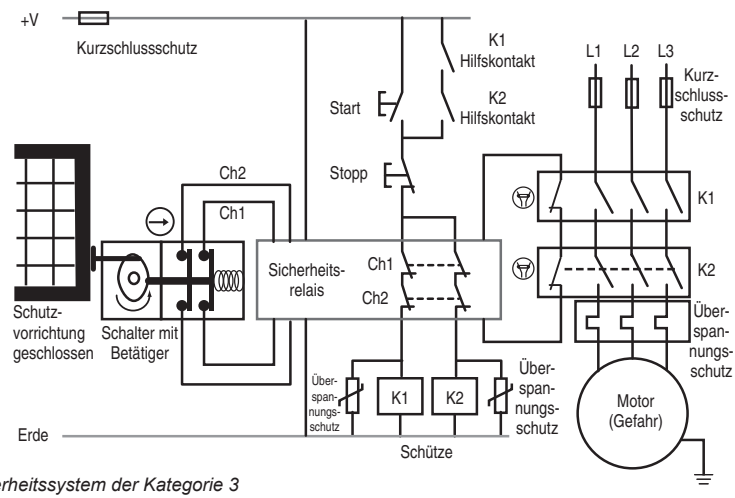
Kategorie 3

Für Kategorie 3 müssen nicht nur die Anforderungen von Kategorie B erfüllt und bewährte Sicherheitsprinzipien angewandt werden. Darüber hinaus muss beim Vorliegen eines einzigen Fehlers auch die Sicherheitsfunktion erfolgreich ausgeführt werden können. Der Fehler muss bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden (sofern dies auf vernünftige, praktikable Weise möglich ist).

Auch hier findet sich die Formulierung „auf einigermaßen praktikable Weise“ wieder. Dies gilt auch für Fehler, die eventuell nicht erkannt werden können. Sofern der unerkennbare Fehler nicht zum Ausfall der Sicherheitsfunktion führt, kann die Sicherheitsfunktion die Anforderungen von Kategorie 3 erfüllen. Eine Anhäufung unerkannter Fehler kann daher zum Ausfall der Sicherheitsfunktion führen.



Dieses Blockdiagramm veranschaulicht die Prinzipien eines Systems der Kategorie 3. Redundanz in Verbindung mit übergreifender Überwachung auf einigermaßen praktikable Weise und eine Überwachung der Ausgänge gewährleisten die Leistungsfähigkeit des Sicherheitssystems.



Sicherheitssystem der Kategorie 3

Dieses Beispiel zeigt ein System der Kategorie 3. Der Sicherheitsschalter mit Betätiger wird um redundant ausgelegte Kontakte erweitert. Im Innern enthält das Sicherheitsrelais redundante Schaltkreise, die sich gegenseitig überwachen. Redundant ausgelegte Schütze unterbrechen die Stromzufuhr vom Motor. Die Schütze werden vom Sicherheitsrelais über auf einigermaßen praktikable Weise mechanisch verbundene Kontakte überwacht.

Die Fehlererkennung muss für jedes Teil des Sicherheitssystems und für die Verbindungen (also das System) berücksichtigt werden. Welche Ausfallmodi sind bei einem zweikanaligen Schalter mit Betätiger verfügbar? Welche Ausfallmodi sind beim Sicherheitsrelais vorhanden? Welche Ausfallmodi bestehen bei den Schützen K1 und K2? Welche Ausfallmodi stellt die Verdrahtung bereit?

Der Sicherheitsschalter mit Betätiger wurde mit Direktöffnerkontakten konzipiert. Daher ist bekannt, dass beim Öffnen der Schutztür ein verschweißter Kontakt geöffnet wird. So wird ein Ausfallmodus gelöst. Sind andere Ausfallmodi verfügbar?

Der Direktöffnerschalter ist in der Regel mit einer Federrückführung ausgestattet. Falls der Kopf abgenommen oder abgebrochen wird, federn die Sicherheitskontakte zurück in die geschlossene (sichere) Position. Viele Verriegelungsschalter verfügen über abnehmbare Köpfe, um den Installationsanforderungen der unterschiedlichsten Anwendungen gerecht zu werden. Der Kopf kann abgenommen und zwischen zwei bis vier Positionen gedreht werden.

Ein Ausfall könnte auftreten, wenn die Montageschrauben des Kopfs nicht ordnungsgemäß angezogen sind. Unter diesen Umständen kann die erwartete Vibration der Maschine dazu führen, dass sich die Montageschrauben herausdrehen. Der Schaltkopf mit Federdruck nimmt

den Druck von den Sicherheitskontakten, woraufhin die Sicherheitskontakte schließen. Folglich werden beim Öffnen der Schutztür nicht die Sicherheitskontakte geöffnet, und es kommt zu einem Ausfall bei Gefahr.

Auf ähnliche Weise muss der Schaltmechanismus im Schalter überprüft werden. Wie wahrscheinlich ist es, dass der Ausfall einer Komponente zum Ausfall der Sicherheitsfunktion führt? Gängige Praxis ist der Einsatz von Sicherheitsschaltern mit Betätiger und zwei Kontakten in Schaltkreisen der Kategorie 3. Bei dieser Verwendung muss ausgeschlossen sein, dass ein einziger Ausfall des Schalters zum Öffnen der Sicherheitskontakte führt. Man spricht dabei von „Fehlerausschluss“, der weiter hinten in diesem Kapitel näher beschrieben wird.

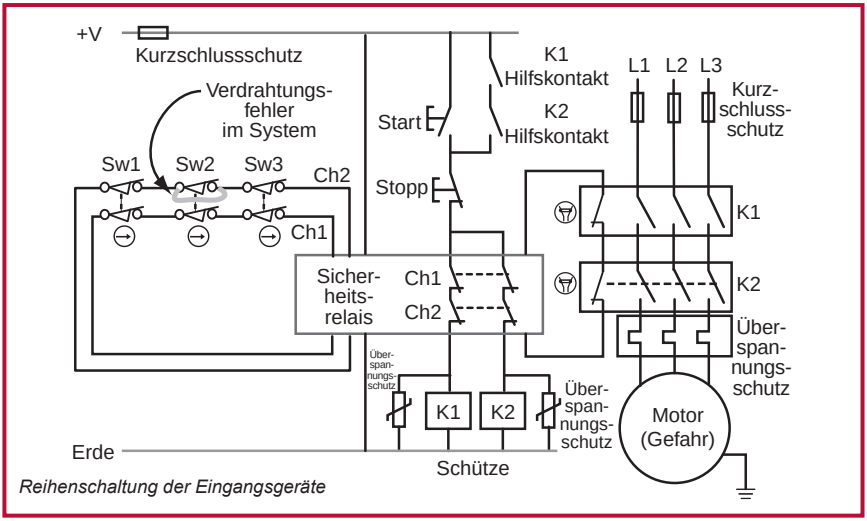
Ein Sicherheitsrelais wird oft durch Dritte beurteilt und einer Kategorie (und/oder einem PL und SIL CL) zugeordnet. Das Sicherheitsrelais umfasst oft eine zweikanalige Funktion, eine kanalübergreifende Überwachung, die Überwachung externer Geräte und einen Kurzschlussschutz. Es wurden noch keine speziellen Normen mit Anleitungen zum Bau oder zur Verwendung von Sicherheitsrelais verfasst. Sicherheitsrelais werden daraufhin überprüft, ob sie die Sicherheitsfunktion gemäß EN ISO 13849-1 oder gemäß der auslaufenden Norm EN 954-1 erfüllen. Die Klassifizierung des Sicherheitsrelais muss identisch oder höher sein wie die erforderliche Klassifizierung des Systems, in dem es verwendet wird.

Zwei Schütze sollen gewährleisten, dass die Ausgangsgeräte die Sicherheitsfunktion ausführen können. Mit Überlast- und Kurzschlussschutz ist die Wahrscheinlichkeit eines Schützausfalls mit verschweißten Kontakten gering, doch nicht ausgeschlossen. Ein Schütz kann auch dann ausfallen, wenn seine Kontakte zur Leistungsschaltung aufgrund eines festsitzenden Ankers geschlossen bleiben. Wenn ein Schütz ausfällt und zu einer gefährlichen Situation führt, unterbricht das zweite Schütz die Stromversorgung der Gefahrenquelle. Das Sicherheitsrelais erkennt das fehlerhafte Schütz beim nächsten Maschinenzyklus. Wenn die Schutztür geschlossen ist und die Starttaste gedrückt wird, bleiben die mechanisch verbundenen Kontakte des fehlerhaften Schützes geöffnet, und das Sicherheitsrelais kann seine Sicherheitskontakte nicht schließen, wodurch der Fehler erkannt wird.

Unerkannte Fehler

Mit einer Systemstruktur der Kategorie 3 können einige Fehler auftreten, die nicht erkannt werden. Sie dürfen jedoch alleine nicht zum Ausfall der Sicherheitsfunktion führen.

Wenn Fehler erkannt werden können, ist zu beachten, dass sie unter bestimmten Umständen entweder maskiert oder unbeabsichtigt durch den Betrieb anderer Geräte innerhalb der Systemstruktur gelöscht werden könnten.



Reihenschaltung der Eingangsgeräte

Diese Abbildung zeigt einen häufig verwendeten Ansatz zum Anschließen mehrerer Geräte an ein Überwachungs-Sicherheitsrelais. Jedes Gerät enthält zwei Öffnerkontakte mit Direktöffnung. Bei diesen Geräten kann es sich um eine Mischung aus Verriegelungen oder Not-Halt-Tastern handeln. Dieser Ansatz sorgt für geringere Verdrahtungskosten, da die Eingangsgeräte in einer Prioritätskette angeschlossen werden. Angenommen, es tritt an einem der Kontakte an Sw2 ein Kurzschlussfehler auf (siehe Abbildung). Kann dieser Fehler erkannt werden?

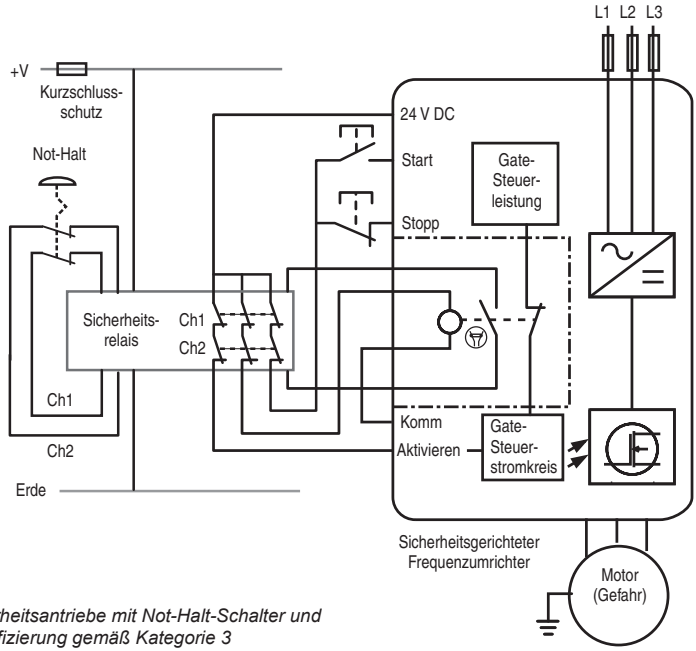
Wenn der Schalter Sw1 (oder Sw3) geöffnet ist, sind Ch1 und Ch2 offene Schaltkreise und das Sicherheitsrelais unterbricht die Stromversorgung zur Gefahrenquelle. Beim anschließenden Öffnen und Schließen von Sw3 wird der Fehler an seinen Kontakten nicht erkannt, weil am Sicherheitsrelais keine Statusänderung auftritt: Ch1 und Ch2 bleiben beide geöffnet. Wenn Sw1 (oder Sw3) anschließend geschlossen werden, kann die Gefahr durch Drücken der START-Taste neu gestartet werden. Unter diesen Umständen führte der Fehler nicht zu einem Ausfall der Sicherheitsfunktion, doch er wurde nicht erkannt. Er verbleibt im System und ein nachfolgender Fehler (ein Kurzschluss am zweiten Kontakt von Sw2) könnte zum Verlust der Sicherheitsfunktion führen.

Wenn nur Sw2 geöffnet und geschlossen wird und die anderen Schalter nicht betätigt werden, öffnet Ch1 und Ch2 bleibt geschlossen. Das Sicherheitsrelais schaltet die Gefahrenquelle aus, da Ch1 geöffnet ist. Wenn Sw2 schließt, kann der Motor beim Drücken der Starttaste nicht gestartet werden, da Ch2 nicht geöffnet werden konnte. Der Fehler wird erkannt. Wenn jedoch aus irgendeinem Grund Sw1 (oder Sw3) anschließend geöffnet und geschlossen wird, sind Ch1 und Ch2 zunächst geöffnete und anschließend geschlossene Schaltkreise. Diese Abfolge simuliert das Löschen des Fehlers und führt zu einer unbeabsichtigten Rückstellung am Sicherheitsrelais.

Dies wirft die Frage auf, welcher Diagnosedeckungsgrad (DC) für die einzelnen Schalter innerhalb dieser Struktur in Anspruch genommen werden kann, wenn EN ISO 13849-1 oder IEC 62061 angewandt werden. Zum Zeitpunkt der Veröffentlichung dieses Textes gab es keine eindeutigen Anleitungen dazu. Doch es ist üblich und angemessen, einen DC von 60 % vorauszusetzen, wenn die Schalter in geeigneten Abständen einzeln auf Fehler überprüft werden. Wenn es vorhersehbar ist, dass einer (oder mehrere) der Schalter niemals einzeln getestet wird, kann argumentiert werden, dass sein DC als null beschrieben werden soll. Zum Zeitpunkt der Veröffentlichung dieses Textes wird die Norm EN ISO 13849-2 gerade überarbeitet. Nach ihrer Veröffentlichung stellt sie eventuell weitere Informationen zu diesem Thema zur Verfügung.

Die Reihenschaltung mechanisch verbundener Kontakte ist auf Kategorie 3 beschränkt, da sie zum Ausfall der Sicherheitsfunktion aufgrund einer Anhäufung von Fehlern führen kann. In praktischer Hinsicht würde die Verringerung des DC (und daher des SFF) den maximal erreichbaren PL- und SIL-Wert auf PLd und SIL2 begrenzen.

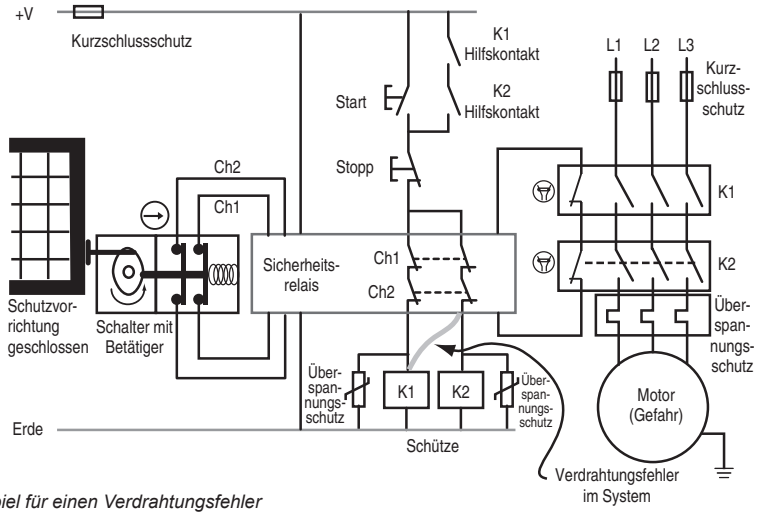
Interessant ist, dass diese Merkmale einer Struktur der Kategorie 3 schon immer berücksichtigt werden mussten, doch erst durch die neueren Normen zur funktionalen Sicherheit nähere Beachtung fanden.



Sicherheitsantriebe mit Not-Halt-Schalter und Klassifizierung gemäß Kategorie 3

Diese Abbildung zeigt einen Schaltkreis der Kategorie 3, der einen sicherheitsgerichteten Frequenzumrichter verwendet. Entwicklungen in der Antriebstechnologie erlauben in Kombination mit der Aktualisierung der Normen EN/IEC 60204-1 und NFPA 79 den Einsatz sicherheitsgerichteter Antriebe in Not-Halt-Stromkreisen, ohne dafür eine elektromechanische Trennung des Aktors (z. B. des Motors) zu benötigen.

Durch Drücken des Not-Halt-Schalters werden die Ausgänge des Sicherheitsrelais geöffnet. Dabei wird ein Stoppsignal an den Antrieb gesendet, das Aktivierungssignal entfernt und die Steuerspannung zur Tür geöffnet. Der Antrieb führt einen Stopp der Kategorie 0 aus – sofortige Unterbrechung der Stromversorgung des Motors. Diese Funktion wird auch „Safe Torque Off“ (sicherheitsgerichtete Drehmomentabschaltung) genannt. Der Antrieb entspricht Kategorie 3, da er mithilfe redundanter Signale die Stromversorgung des Motors unterbricht: mit dem Aktivierungssignal und mit dem Signal eines positiv angesteuerten Relais. Das positiv angesteuerte Relais sendet an den Aktor ein einigermaßen praktikables Feedback. Der Antrieb selbst wird analysiert, wodurch überprüft wird, dass ein einziger Fehler nicht zum Ausfall der Sicherheitsfunktion führen kann.

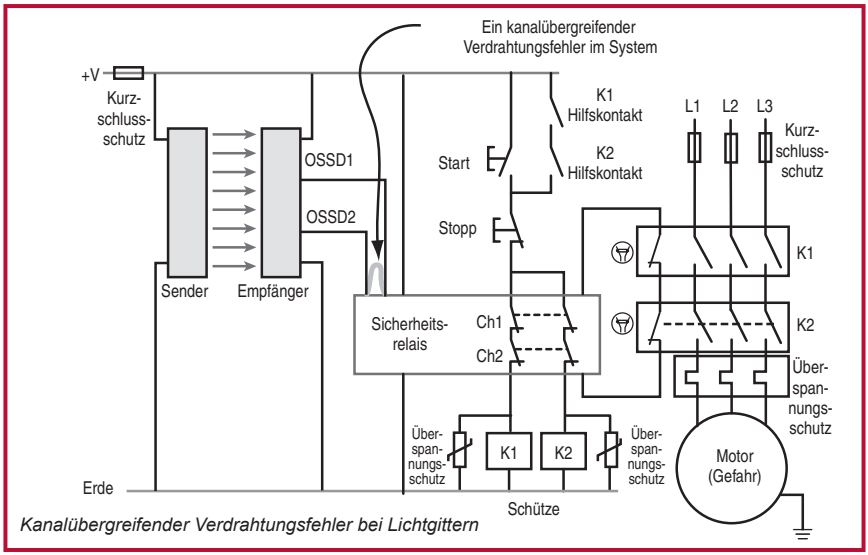


Beispiel für einen Verdrahtungsfehler

Die Abbildung zeigt ein Beispiel für einen Verdrahtungsfehler, einen Kurzschluss, vom Sicherheitsausgang von Kanal 2 des Sicherheitsrelais zur Spule von Schütz K1. Alle Komponenten funktionieren ordnungsgemäß. Dieser Verdrahtungsfehler kann vor der Inbetriebnahme der Maschine oder zu einem späteren Zeitpunkt während der Wartung oder während Erweiterungen auftreten.

Kann dieser Fehler erkannt werden?

Dieser Fehler kann, wie dargestellt, nicht vom Sicherheitssystem erkannt werden. Glücklicherweise führt er alleine nicht zum Ausfall der Sicherheitsfunktion. Dieser Fehler, ebenso wie der Fehler von Ch1 zu K2, muss während der Inbetriebnahme oder bei den Prüfungen nach Wartungsarbeiten erkannt werden. Die Liste der möglichen Fehlerausschlüsse in der Norm EN ISO 13849-2, Anhang D, Tabelle D4, verdeutlicht, dass diese Fehlertypen ausgeschlossen werden können, wenn die Geräte in einem Elektrogehäuse montiert werden und das Gehäuse sowie die Verdrahtung mit den Anforderungen der Norm IEC/EN 60204-1 konform sind. Der gemeinsame technische Bericht zu EN ISO 13849-1 und IEC 62061 verdeutlicht ebenfalls, dass dieser Fehlerausschluss bis einschließlich PLe und SIL3 in Betracht gezogen werden kann. Er kann auch für Kategorie 4 verwendet werden.



Kanalübergreifender Verdrahtungsfehler bei Lichtgittern

Dieses Beispiel zeigt ein Sicherheitssystem mit Lichtgittern (OSSD-Ausgänge)

Kann das Sicherheitssystem diesen Fehler erkennen?

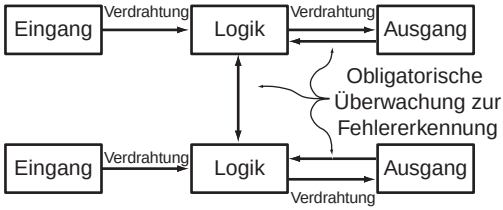
Das Überwachungs-Sicherheitrelais kann diesen Fehler nicht erkennen, da beide Eingänge nach +V gezogen werden. In diesem Beispiel wird der Verdrahtungsfehler vom Lichtgitter erkannt. Einige Lichtgitter verwenden als Fehlererkennungstechnik sogenannte „Impulstests". Bei diesen Lichtgittern wird der Fehler sofort erkannt, woraufhin das Lichtgitter seinen Ausgang ausschaltet. In anderen Beispielen wird der Fehler erkannt, wenn die Schutzfunktion des Lichtgitters aufgehoben wird. Wenn das Lichtgitter versucht, seinen Ausgang einzuschalten, wird der Fehler erkannt und der Ausgang bleibt ausgeschaltet. In beiden Fällen bleibt die Gefahrenquelle deaktiviert, solange der Fehler vorliegt.

Fehlererkennung durch Impulstests

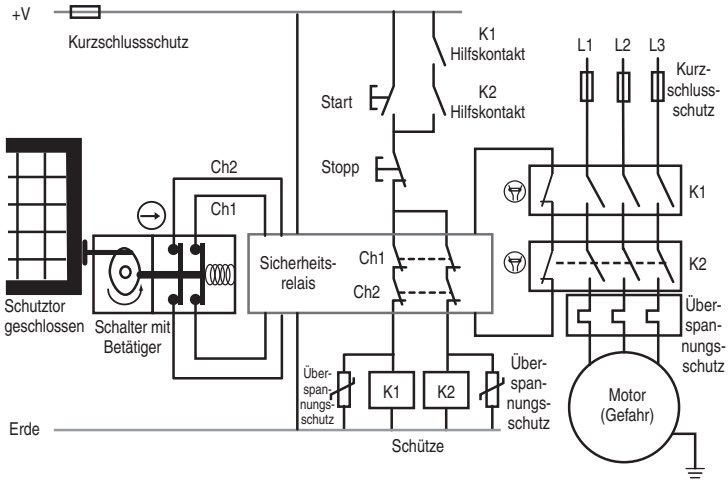
Sicherheitsschaltkreise sind so konzipiert, dass sie Strom führen, wenn das Sicherheitssystem aktiv und die Gefahrenquelle geschützt ist. Bei Impulstests fällt der Schaltkreisstrom für sehr kurze Zeit auf null. Diese Zeitspanne ist für den Sicherheitsschaltkreis zu kurz, um zu reagieren und die Gefahrenquelle zu deaktivieren. Allerdings ist sie für ein mikroprozessorbasiertes System lang genug, um den Fehler zu erkennen. Die Impulse in den Kanälen erfolgen zeitversetzt. Wenn ein fehlerübergreifender Kurzschluss eintritt, erkennt der Mikroprozessor die Impulse in beiden Kanälen und gibt einen Befehl zum Deaktivieren der Gefahrenquelle aus.

Kategorie 4

Genau wie Kategorie 3 erfordert auch Kategorie 4, dass das Sicherheitssystem die Anforderungen von Kategorie B erfüllt, Sicherheitsprinzipien anwendet und die Sicherheitsfunktion ausführt, sofern ein einzelner Fehler vorliegt. Im Gegensatz zu Kategorie 3, bei der eine Anhäufung von Fehlern zum Ausfall der Sicherheitsfunktion führen kann, erfordert Kategorie 4, dass die Sicherheitsfunktion auch bei einer Anhäufung von Fehlern ausgeführt werden kann. Wenn es um die Anhäufung von Fehlern geht, reichen eventuell zwei Fehler aus, wobei manche Konfigurationen auch drei Fehler erfordern.



Dieses Beispiel zeigt ein Blockdiagramm für Kategorie 4. Die Überwachung beider Ausgangsgeräte und die übergreifende Überwachung ist grundsätzlich erforderlich (also nicht nur, wenn es auf vernünftige Weise praktikabel ist). So kann Kategorie 4 ganz einfach von Kategorie 3 unterschieden werden.

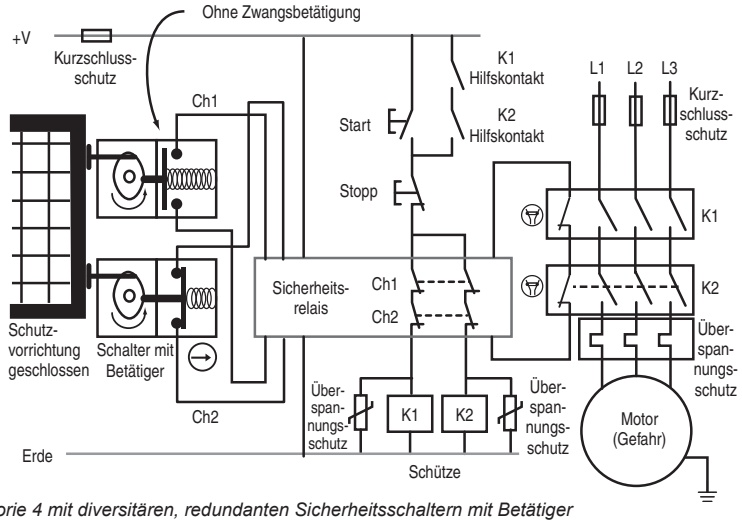


Kategorie 4 mit Fehlerausschluss beim Sicherheitsschalter mit Betätiger

Dieses Beispiel zeigt einen Schaltkreis der Kategorie 4 mit Fehlerausschluss am Sicherheitsschalter mit Betätiger. Durch den Fehlerausschluss entfällt die Überlegung, was geschieht, wenn die Kontakte des Sicherheitsschalters mit Betätiger nicht öffnen. Der Fehlerausschluss muss technisch gerechtfertigt und dokumentiert sein. Bei der Rechtfertigung sind Aktorgeschwindigkeit, Aktorausrichtung, mechanische Stopps und ein sicherer Schaltkopf zu berücksichtigen.

Wenn es der Entwickler des Sicherheitssystems vorzieht, Verriegelungen mit Betätiger zu verwenden, er jedoch Zweifel hinsichtlich der Verwendung des Fehlerausschlusses bei den Verriegelungen hat, können zwei Sicherheitsschalter mit Betätiger eingesetzt werden, um die Anforderungen von Kategorie 4 zu erfüllen. Das Sicherheitsrelais selbst muss für Kategorie 4 klassifiziert sein, und beide Ausgangsschütze, die mechanisch verbundene Kontakte verwenden, müssen überwacht werden.

Durch Diversität kann die Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion aufgrund von Fehlern mit gleichem Modus oder gemeinsamer Ursache verringert werden. Einer der Sicherheitsschalter mit Betätiger kann in den negativen Modus konvertiert werden. Es ist ein im negativen Modus arbeitender Schalter zulässig, vorausgesetzt, ein zweiter Schalter verwendet direkt öffnende Kontakte. Die folgende Abbildung zeigt ein Beispiel für dieses diversitäre Konzept. Bei diesem Konzept muss das Sicherheitsrelais so konzipiert sein, dass es Schließer- und Öffnereingänge akzeptiert.



Kategorie 4 mit diversitären, redundanten Sicherheitsschaltern mit Betätiger

Komponenten- und Systemklassifizierungen

Kategorien können als Teil der Klassifizierung von Sicherheitskomponenten (Geräten) sowie als Klassifizierung von Systemen verwendet werden. Dies führt zu einiger Verwirrung, die jedoch bei näherer Betrachtung der Komponenten und deren Fähigkeiten beseitigt werden kann. Bei näherer Betrachtung der obigen Beispiele werden Sie feststellen, dass eine Komponente, wie beispielsweise ein Verriegelungsschalter der Kategorie 1 alleine in einem System der Kategorie 1 eingesetzt werden kann. Zudem kann er in einem System der Kategorie 2 verwendet werden, wenn eine zusätzliche Funktionsüberwachung zur Verfügung

steht. Er kann darüber hinaus als Teil eines Systems der Kategorie 3 oder 4 eingesetzt werden, wenn zwei der Komponenten zusammen mit einer Diagnosefunktion verwendet werden, die über ein Sicherheitsrelais bereitgestellt wird.

Einige Komponenten, wie z. B. Sicherheitsrelais und programmierbare Sicherheitssteuerungen verfügen über ihre eigenen internen Diagnosefunktionen und überprüfen sich selbst, um eine ordnungsgemäße Leistung sicherzustellen. Daher können sie als Sicherheitskomponenten eingestuft werden, die die Anforderungen der Kategorien 2, 3 oder 4 ohne zusätzliche Maßnahmen erfüllen.

Fehlerüberlegungen und -ausschlüsse

Sicherheitsanalysen erfordern eine umfassende Fehleranalyse. Außerdem muss grundsätzlich klar sein, wie das Sicherheitssystem beim Vorhandensein von Fehlern reagiert. ISO 13849-1 und ISO 13849-2 enthalten Details zu den Fehlerüberlegungen und Fehlerausschlüssen.

Wenn ein Fehler zum Ausfall einer nachfolgenden Komponente führt, gelten der erste Fehler und alle nachfolgenden Fehler als ein Fehler.

Wenn zwei oder mehr Fehler als Folge einer einzelnen Ursache auftreten, gelten die Fehler als ein Fehler. Dies sind sogenannte Fehler aufgrund gemeinsamer Ursache.

Das Auftreten von zwei oder mehr Fehlern zur gleichen Zeit gilt als äußerst unwahrscheinlich und wird in dieser Analyse nicht berücksichtigt. Grundsätzlich wird davon ausgegangen, dass nur ein Fehler zwischen den Anforderungen an die Sicherheitsfunktion auftritt, sofern die Zeiträume zwischen der Verwendung der Funktion nicht zu groß sind.

Fehlerausschlüsse

Die auslaufende Norm EN 954-1 und die neueren Normen EN ISO 13849-1 und IEC 62061 lassen alle die Verwendung von Fehlerausschlüssen zu, wenn die Klassifizierung eines Sicherheitssystems bestimmt wird, sofern dargelegt werden kann, dass das Auftreten des Fehlers äußerst unwahrscheinlich ist. Es ist wichtig, dass bei der Anwendung von Fehlerausschlüssen diese ordnungsgemäß gerechtfertigt werden und dass sie für die vorgesehene Einsatzzeit des Sicherheitssystems gültig sind. Je höher das Risiko, vor dem das Sicherheitssystem schützen soll, desto besser muss die Rechtfertigung des Fehlerausschlusses sein. Bei bestimmten Fehlerausschlusstypen hat dies stets zu einiger Verwirrung hinsichtlich der Tatsache geführt, wann bestimmte Fehlerausschlusstypen verwendet oder nicht verwendet werden können. Wie bereits in diesem Kapitel verdeutlicht, wurden durch die neuesten Normen und Anleitungsdokumente einige Aspekte dieses Problems bereits geklärt.

Im Allgemeinen darf man sich, wenn PLe oder SIL3 für eine von einem Sicherheitssystem implementierte Sicherheitsfunktion angegeben ist, nicht allein auf Fehlerausschlüsse verlassen, um diesen Performance Level zu erreichen. Dies hängt von der verwendeten Technologie und der vorgesehenen Betriebsumgebung ab. Daher ist es wichtig, dass der Entwickler bei der Verwendung von Fehlerausschlüssen umso vorsichtiger vorgeht, je höher diese PL- oder

SIL-Anforderung ist. Beispielsweise ist der Fehlerausschluss nicht auf mechanische Aspekte elektromechanischer Positionsschalter und manuell betätigter Schalter (z. B. Not-Halt-Geräte) anwendbar, wenn ein PLe- oder SIL3-System angestrebt wird. Fehlerausschlüsse, die auf bestimmte mechanische Fehlerzustände angewandt werden können (z. B. Verschleiß/Korrosion, Brüche), sind in Tabelle A.4 der Norm ISO 13849-2 beschrieben. Daher muss ein Schutztor-Zuhaltungssystem, das PLe oder SIL3 erzielen muss, über eine minimale Fehlertoleranz von 1 (z. B. zwei konventionelle mechanische Positionsschalter) verfügen, um diesen Performance Level zu erreichen, da normalerweise der Ausschluss von Fehlern wie gebrochene Schalterbetätiger nicht zu rechtfertigen ist. Es ist jedoch eventuell akzeptabel, Fehler auszuschließen, wie z. B. einen Verdrahtungskurzschluss innerhalb eines Schaltschranks, der in Übereinstimmung mit relevanten Industrienormen entwickelt wurde.

Weitere Informationen zur Anwendung von Fehlerausschlüssen finden Sie in der bevorstehenden Überarbeitung der Norm EN ISO 13849-2.

Ausschaltkategorien gemäß IEC/EN 60204-1 und NFPA 79

Es ist bedauerlich und verwirrend, dass der Begriff „Kategorie“ hinsichtlich sicherheitsbezogener Steuerungssysteme zwei unterschiedliche Bedeutungen hat. Bisher wurden die Kategorien näher erläutert, die aus der Norm EN 954-1 stammen. Sie stellen eine Klassifizierung der Leistung eines Sicherheitssystems unter Fehlerbedingungen dar.

Darüber hinaus gibt es eine als „Ausschaltkategorie“ bekannte Klassifizierung, die aus IEC/EN 60204-1 und NFPA 79 stammt. Es gibt drei Ausschaltkategorien.

Ausschaltkategorie 0 erfordert die unmittelbare Unterbrechung der Energieversorgung der Aktoren. Dies wird manchmal auch als unkontrollierter Stopp bezeichnet, weil es unter bestimmten Umständen einige Zeit dauern kann, bis die Bewegung zum Stillstand kommt, da der Motor bis zum Stillstand ausläuft.

Ausschaltkategorie 1 erfordert, dass die Energieversorgung beibehalten wird, um einen Bremsvorgang bis zum Stopp zu aktivieren. Anschließend muss die Energieversorgung des Aktors unterbrochen werden.

Ausschaltkategorie 2 erfordert die unmittelbare Unterbrechung der Energieversorgung der Aktoren.

Es können nur die Ausschaltkategorien 0 oder 1 als Not-Halt verwendet werden. Welche der beiden Kategorien eingesetzt wird, muss durch eine Risikobeurteilung bestimmt werden.

Für alle bisher dargestellten Schaltkreisbeispiele in diesem Kapitel wurde die Ausschaltkategorie 0 verwendet. Die Ausschaltkategorie 1 wird mit einem zeitverzögerten Ausgang für die endgültige Unterbrechung der Energieversorgung erzielt. Eine Schutzgitterverriegelung mit Verriegelungsschalter ist oft Teil eines Stoppsystems der Kategorie 1. Auf diese Weise bleibt die Schutztür in der geschlossenen Position verriegelt, bis die Maschine einen sicheren Zustand erreicht hat (z. B. bis sie zum völligen Stillstand gekommen ist).

Wird eine Maschine gestoppt, ohne die speicherprogrammierbare Steuerung ordnungsgemäß zu berücksichtigen, führt dies möglicherweise zu einem Neustart, was schwere Werkzeug- und Maschinenschäden zur Folge haben kann. Für eine sicherheitsbezogene Stoppaufgabe darf man sich nicht auf eine Standard-SPS (also keine Sicherheits-SPS) allein verlassen. Daher müssen andere Konzepte in Betracht gezogen werden.

Im Folgenden werden zwei mögliche Lösungen vorgestellt:

1. Sicherheitsrelais mit zeitverzögertem Überbrückungsbefehl

Es wird ein Sicherheitsrelais mit unmittelbaren und verzögerten Ausgängen verwendet. Die unmittelbar handelnden Ausgänge sind mit den Eingängen am programmierbaren Gerät (z. B. der SPS) verbunden, während die verzögert handelnden Ausgänge am Schütz angeschlossen sind. Wenn der Verriegelungsschalter der Schutzvorrichtung betätigt wird, schalten die unmittelbaren Ausgänge am Sicherheitsrelaisschalter sofort. Das programmierbare System veranlasst daraufhin eine korrekt ablaufende Ausschaltsequenz. Nachdem eine kurze, doch hierfür ausreichende Zeit verstrichen ist, schaltet der verzögerte Ausgang am Sicherheitsrelais und trennt das Hauptschütz.

Hinweis: Berechnungen zum Bestimmen der Gesamtanhaltezeit müssen die Verzögerungszeit des Sicherheitsrelais berücksichtigen. Dies ist besonders wichtig, wenn dieser Faktor die Anordnung von Geräten gemäß der Berechnung des Sicherheitsabstands bestimmt.

2. Sicherheits-SPS

Die erforderlichen Logik- und Zeitmessfunktionen können bequem über eine (Sicherheits-) SPS mit einer entsprechenden SIL-Klassifizierung implementiert werden. In der Praxis könnte dies durch Verwendung einer Sicherheits-SPS erzielt werden, wie z. B. SmartGuard oder GuardLogix.

Anforderungen an Sicherheitssteuerungssysteme in den USA

In den USA gibt es zahlreiche Normen, die sich mit den Anforderungen an sicherheitsbezogene Steuerungssysteme befassen. Dabei sind zwei Dokumente von besonderer Bedeutung: ANSI B11.TR3 und ANSI R15.06. Der technische Bericht ANSI B11.TR3 definiert vier Stufen, die durch das erwartete Ausmaß der Risikominderung charakterisiert sind, die die einzelnen Stufen ermöglichen: Die Anforderungen für die einzelnen Stufen sind im Folgenden definiert.

Niedrigste Stufe

Gemäß der Norm ANSI B11.TR3 umfassen Schutzeinrichtungen, die die niedrigste Stufe einer Risikominderung zur Verfügung stellen, elektrische, elektronische, hydraulische oder pneumatische Geräte sowie zugeordnete Steuerungssysteme mit einer Einkanal-Konfiguration. Bei diesen Anforderungen wird davon ausgegangen, dass sicherheitsbezogene Geräte verwendet werden. Dies entspricht im Wesentlichen den Anforderungen von Kategorie 1 der Norm ISO 13849-1.

Geringe/mittlere Risikominderung

Die in der Norm ANSI B11.TR3 genannten Schutzeinrichtungen, die eine geringe/mittlere Risikominderung bieten, umfassen Steuerungssysteme mit Redundanz, die manuell überprüft werden können, um die Leistung des Sicherheitssystems sicherzustellen. Werden die Anforderungen allein betrachtet, umfasst das System eine einfache Redundanz. Die Verwendung einer Prüffunktion ist nicht erforderlich. Ohne die Überprüfung kann eine der redundanten Sicherheitskomponenten ausfallen, wobei das Sicherheitssystem dies nicht erkennen würde. Das Ergebnis wäre ein einkanaliges System. Die Stufe dieser Risikominderung kann am besten mit Kategorie 2 verglichen werden, wenn eine Überprüfung eingesetzt wird.

Hohe/mittlere Risikominderung

Schutzeinrichtungen, die gemäß der Norm ANSI B11.TR3 eine hohe/mittlere Risikominderung bieten, umfassen Steuerungssysteme mit Redundanz und Eigenüberwachung beim Start, die die Leistung des Sicherheitssystems sicherstellen. Bei Maschinen, die jeden Tag gestartet werden, bietet die Eigenüberwachung eine erhebliche Verbesserung der Sicherheitsintegrität gegenüber den Systemen, die lediglich eine Redundanz aufweisen. Für Maschinen, die rund um die Uhr (24/7) laufen, stellt die Eigenüberwachung allenfalls eine geringe Verbesserung dar. Durch eine periodische Überwachung des Sicherheitssystems werden die Anforderungen an Kategorie 3 ausgerichtet.

Höchste Stufe der Risikominderung

ANSI B11.TR3 bietet die höchste Risikominderung durch Steuerungssysteme mit Redundanz und kontinuierlicher Eigenüberwachung. Die Eigenüberwachung muss die Leistung des Sicherheitssystems verifizieren. Die Herausforderung für die Entwickler des Sicherheitssystems besteht darin, die Bedeutung des Worts „kontinuierlich“ zu bestimmen. Viele Sicherheitssysteme führen ihre Prüfungen beim Start aus, wenn eine Anforderung an das Sicherheitssystem gerichtet wird.

Auf der anderen Seite führen einige Komponenten eine kontinuierliche Eigenüberwachung durch. Lichtgitter beispielsweise schalten ihre LEDs nacheinander ein und aus. Wenn ein Fehler auftritt, schaltet das Lichtgitter seine Ausgänge aus, bevor eine Anforderung an das Sicherheitssystem gerichtet wird, da die Eigenüberwachung kontinuierlich stattfindet. Auf Mikroprozessoren basierende Relais und Sicherheits-SPS sind weitere Komponenten, die eine kontinuierliche Eigenüberwachung durchführen.

Die Anforderung des Steuerungssystems an eine „kontinuierliche“ Eigenüberwachung soll die Auswahl der Komponenten nicht auf Lichtgitter und mikroprozessorbasierte Logikeinheiten beschränken. Die Überprüfung muss beim Start und nach jeder Anforderung an das Sicherheitssystem stattfinden. Diese Stufe der Risikominderung dient zur Ausrichtung an Kategorie 4 der Norm ISO 13849-1.

Roboternormen: USA und Kanada

Die Roboternormen in den USA (ANSI RIA R15.06) und Kanada (CSA Z434-03) sind relativ ähnlich. Beide bestehen aus vier Stufen, die mit den Kategorien der Norm EN 954-1:1996 vergleichbar sind. Diese werden im Folgenden beschrieben.

Einfach

Auf dieser untersten Stufe müssen einfache Sicherheitssteuerungssysteme entwickelt und gebaut werden, die über eine akzeptable, einkanalige Schaltung verfügen. Außerdem können diese Systeme programmierbar sein. In Kanada ist diese Stufe weiter eingeschränkt und darf nur für Signal- und Meldungszwecke verwendet werden. Die Herausforderung für die Entwickler des Sicherheitssystems besteht darin, die Bedeutung des Worts „akzeptabel“ zu bestimmen. Was ist eine akzeptable, einkanalige Schaltung? Für wen ist das System akzeptabel? Diese einfache Kategorie lässt sich am besten mit Kategorie B der Norm EN 954-1:1996 vergleichen.

Einkanalig

Die nächste Stufe ist ein einkanaliges Sicherheitssteuerungssystem, das folgende Merkmale aufweist:

- Es ist hardwarebasiert oder ein sicherheitsbezogenes Software-/Firmwaregerät.
- Es umfasst sicherheitsbezogene Komponenten.
- Es wird in Übereinstimmung mit den Empfehlungen des Herstellers eingesetzt.
- Es verwendet bewährte Schaltkreisaufbauten.

Ein Beispiel für einen bewährten Schaltkreisaufbau ist ein einkanaliges, elektromechanisches, positives Unterbrechungsgerät, das im ausgeschalteten Zustand einen Stopp signalisiert. Da es ein einkanaliges System ist, kann der Ausfall einer einzigen Komponente zum Ausfall der Sicherheitsfunktion führen. Diese einfache Kategorie kann am besten mit Kategorie 1 der Norm EN 9541:1996 verglichen werden.

Sicherheitsbezogenes Software-/Firmwaregerät

Zwar waren bisher hardwarebasierte Systeme die bevorzugte Methode zum Bereitstellen von Sicherheitsfunktionen für Roboter, doch werden Software-/Firmwaregeräte immer beliebter, da sie auch mit komplexen Systemen zurechtkommen. Software-/Firmwaregeräte (Sicherheits-SPS oder Sicherheitssteuerungen) sind zulässig, sofern sie sicherheitsbezogen sind. Für diese Klassifikation ist erforderlich, dass der Ausfall einer einzelnen sicherheitsbezogenen Komponente oder ein Firmwareausfall nicht zum Ausfall der Sicherheitsfunktion führt. Wenn der Fehler erkannt wird, muss der nachfolgende automatische Betrieb des Roboters verhindert werden, bis der Fehler behoben wurde.

Um eine Sicherheitsklassifizierung zu erreichen, muss das Software-/Firmwaregerät anhand einer zulässigen Norm durch ein zulässiges Labor getestet werden. In den USA verwaltet die OSHA eine Liste mit national anerkannten Testlabors (NRTL). In Kanada verwaltet der Standards Council of Canada (SCC) eine ähnliche Liste.

Einkanalig mit Überwachung

Einkanalige Sicherheitssteuerungssysteme mit Überwachung müssen die Anforderungen für einkanalige Systeme erfüllen, sicherheitsbezogen sein und Überprüfungen einsetzen. Die Überprüfung der Sicherheitsfunktion(en) muss bei der Inbetriebnahme der Maschine sowie regelmäßig während des Betriebs vorgenommen werden. Die automatische Überprüfung wird gegenüber der manuellen Überprüfung bevorzugt.

Die Überprüfung lässt den Betrieb zu, wenn keine Fehler erkannt werden, oder generiert ein Stoppsignal, wenn ein Fehler erkannt wird. Es muss eine Warnung ausgegeben werden, wenn eine Gefahr auch nach Beendigung der Bewegung weiter besteht. Selbstverständlich darf die Überprüfung selbst nicht zu einer gefährlichen Situation führen. Nach dem Erkennen des Fehlers muss der Roboter in einem sicheren Zustand bleiben, bis der Fehler behoben wurde. Einkanalige Systeme mit Überwachung lassen sich am besten mit Systemen der Kategorie 2 gemäß der Norm EN 954-1:1996 vergleichen.

Steuerungszuverlässigkeit

Die höchste Stufe der Risikominderung in den Roboternormen der USA und von Kanada wird durch sicherheitsbezogene Steuerungssysteme erzielt, die die Anforderungen der Steuerungszuverlässigkeit erfüllen. Sicherheitsgerichete Steuerungssysteme mit Steuerungszuverlässigkeit sind zweikanalige Architekturen mit Überwachung. Die Stoppfunktion des Roboters darf nicht durch den Ausfall einer einzelnen Komponente (einschließlich der Überwachungsfunktion) verhindert werden.

Die Überwachung muss beim Erkennen eines Fehlers einen Stoppbefehl generieren. Bleibt eine Gefahr nach dem Anhalten der Bewegung weiter bestehen, muss ein Warnsignal ausgegeben werden. Das Sicherheitssystem muss in einem sicheren Zustand bleiben, bis der Fehler behoben wurde. Der Fehler wird möglichst zum Zeitpunkt des Ausfalls erkannt. Falls dies nicht möglich ist, muss der Fehler bei der nächsten Anforderung an das Sicherheitssystem erkannt werden. Fehler mit gleichem Modus müssen berücksichtigt werden, wenn es sehr wahrscheinlich ist, dass ein solcher Fehler auftritt.

Die kanadischen Anforderungen unterscheiden sich durch zwei zusätzliche Anforderungen von den Anforderungen in den USA. Zunächst müssen sicherheitsbezogene Steuerungssysteme unabhängig von den normalen Programmsteuerungssystemen sein. Und schließlich darf es nicht möglich sein, das Sicherheitssystem außer Kraft zu setzen oder zu umgehen, ohne dass dies erkannt wird.

Systeme mit Steuerungszuverlässigkeit entsprechen Kategorie 3 und 4 der Norm EN 954-1:1996.

Kommentare zur Steuerungszuverlässigkeit

Der grundlegendste Aspekt der Steuerungszuverlässigkeit ist die Ein-Fehler-Toleranz. Die Anforderungen definieren, wie das Sicherheitssystem beim Auftreten „eines einzelnen Fehlers“, „eines beliebigen einzelnen Fehlers“ oder „eines Ausfalls einer beliebigen einzelnen Komponente“ reagieren muss.

Hinsichtlich der Fehler müssen drei äußerst wichtige Konzepte berücksichtigt werden: (1) Nicht alle Fehler werden erkannt, (2) durch das Wort „Komponente“ werden Fragen zur Verdrahtung aufgeworfen und (3) die Verdrahtung ist ein integrierter Bestandteil des Sicherheitssystems. Verdrahtungsfehler können zum Ausfall einer Sicherheitsfunktion führen.

Zweck der Steuerungszuverlässigkeit ist eindeutig die Leistung der Sicherheitsfunktion beim Vorhandensein eines Fehlers. Wenn der Fehler erkannt wird, muss das Sicherheitssystem eine sichere Aktion ausführen, eine Benachrichtigung zum Fehler ausgeben und den weiteren Betrieb der Maschine so lange verhindern, bis der Fehler korrigiert wurde. Wird der Fehler nicht erkannt, muss die Sicherheitsfunktion weiterhin auf Anforderung ausgeführt werden.

Anwendungsbeispiel mit SISTEMA

Dieses Anwendungsbeispiel veranschaulicht, wie eine Compact GuardLogix-Zugangsabsicherung und PointGuard I/O-Komponenten verdrahtet, konfiguriert und programmiert werden müssen, um ein Sicherheitssystem mit zwei Zonen überwachen zu können. Jede Zone besteht aus einem einzelnen Sicherheitsschalter, der bei seiner Betätigung signalisiert, dass die Stromversorgung zu einem Paar redundanter Schütze für diese Zone unterbrochen werden muss. Dieser Vorgang wird in der zweiten Zone dupliziert. Beide Zonen werden darüber hinaus durch einen globalen Not-Halt-Schalter geschützt, der bei seiner Betätigung ein sicheres Abschalten beider Zonen signalisiert.

Hinweis: Dieses Beispiel dient lediglich der Veranschaulichung. Aufgrund der vielen Variablen und Anforderungen, die mit einer bestimmten Installation verbunden sind, kann Rockwell Automation nicht die Verantwortung oder Haftung für den tatsächlichen Einsatz auf der Grundlage dieses Beispiels übernehmen.

Funktionen und Vorteile

- Compact GuardLogix ermöglicht die Ausführung von Standard- und Sicherheitsanwendungen in einer einzigen Steuerung.
- Standard- und Sicherheits-E/A können in einem einzigen Ethernet-Adapter zusammen vorliegen.
- Sicherheitsstatus und Diagnosen lassen sich problemlos von der Sicherheitsanwendung an die Standardanwendung weiterleiten, um die Anzeige auf der Bedienerschnittstelle zu ermöglichen. Über eine Ethernet-Verbindung ist die dezentrale Weiterleitung an zusätzliche Geräte möglich.
- Die hier beschriebene Anwendung kann erweitert und in die Anwendung eines Kunden integriert werden.

Beschreibung

Diese Anwendung überwacht zwei Zonen. Jede Zone wird durch einen SensaGuard-Sicherheitsschalter geschützt. Wenn eine der beiden Türen geöffnet wird, werden die Ausgangsschütze ausgeschaltet, sodass alle zugeordneten Maschinen für diese Zone heruntergefahren werden. Die Rückstellung erfolgt manuell. Beide Zonen werden darüber hinaus durch einen globalen Not-Halt-Schalter geschützt. Bei Betätigung des Not-Halts werden beide Schützgruppen ausgeschaltet.

Sicherheitsfunktion

Jeder SensaGuard-Sicherheitsschalter ist an einem Paar Sicherheitseingänge eines 1734-IB8S-Moduls angeschlossen (POINTGuard I/O). Die E/A-Module sind über CIP Safety und ein EtherNet/IP-Netzwerk an der Compact GuardLogix-Sicherheitssteuerung (1768-L43S) angeschlossen. Der Sicherheitscode im Sicherheitsprozessor überwacht den Status der Sicherheitseingänge mithilfe eines vorab zertifizierten Sicherheitsbefehls mit dem Namen „DCS“ (Dual

Channel Input Stop). Der Sicherheitscode wird parallel in einer 1oo2-Prozessorkonfiguration ausgeführt. Wenn alle Bedingungen erfüllt sind, wird die Schutztür geschlossen. Es werden keine Fehler an den Eingangsmodulen erkannt, der globale Not-Halt wird nicht betätigt und die Rückstell-Drucktaste wird gedrückt. Ein zweiter zertifizierter Funktionsblock namens „CROUT“ (Configurable Redundant Output) prüft den Status der End-Steuergeräte – einem Paar redundanter 100S-Schütze. Die Steuerung sendet dann ein Ausgangssignal an das 1734-OBS-Modul, um ein Ausgangspaar zu aktivieren, über das die Sicherheitsschütze eingeschaltet werden. Die globale Not-Halt-Funktion wird außerdem durch einen DCS-Befehl überwacht. Beim Betätigen des globalen Not-Halts fährt er beide Zonen herunter.

Stückliste

In diesem Anwendungsbeispiel werden folgende Komponenten eingesetzt:

Bestellnummer	Beschreibung	Anzahl
440N-Z21SS2A	SensaGuard-Schalter Berührungsloser Kunststoff-RFP	2
800FM-G611MX10	800F-Rückstell-Drucktaste – Metall, geschützt, blau, R, Metallkupplungselement, 1 Schließerkontakt, Standard	4
100S-C09ZJ23C	Serie 100S-C – Sicherheitsschütze	2
1768-ENBT	CompactLogix-EtherNet/IP-Bridge-Modul	1
1768-L43S	CompactLogix L43-Prozessor, 2,0 MB Standardspeicher, 0,5 MB Sicherheitsspeicher	1
1768-PA3	Netzteil, 120/240 V AC Eingang, 3,5 A bei 24 V DC	1
1769-ECR	Abschlussmodul/-widerstand, rechts	1
1734-AENT	24-V-DC-Ethernet-Adapter	1
1734-TB	Modulsockel mit abnehmbaren IEC-Schraubklemmen	4
1734-IB8S	Sicherheits-Eingangsmodul	2
1734-OB8S	Sicherheits-Ausgangsmodul	1
1783-US05T	Stratix 2000 Unmanaged Ethernet Switch	1

Konfiguration und Verdrahtung

Ausführliche Informationen zur Installation und Verdrahtung finden Sie in den Produkthandbüchern, die mit den Produkten geliefert werden. Sie können diese auch von der folgenden Webseite herunterladen: http://literature.rockwellautomation.com

Systemüberblick

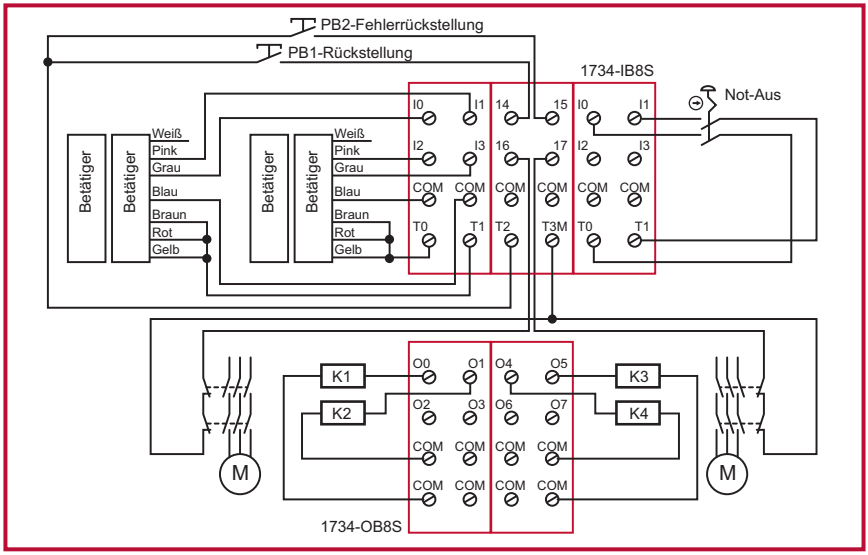
Das 1734-IB8S-Eingangsmodul überwacht die Eingänge beider SensaGuard-Schalter.

Sensaguard verwendet OSSD-Ausgänge, die die Ausgänge regelmäßig testen. So testen die OSSD-Ausgänge die Integrität der Verdrahtung zwischen dem SensaGuard-Schalter und den Sicherheitseingängen.

Die Testimpulsausgänge sind als 24-V-Quellen konfiguriert.

Das End-Steuergerät ist ein Paar 100S-Sicherheitsschütze: K1 und K2. Die Schütze werden vom 1734-OBS-Sicherheitsausgangsmodul gesteuert. Diese sind in einer redundanten Konfiguration verdrahtet und werden beim Einschalten auf Fehler überprüft. Beim Einschalttest wird der Feedbackschaltkreis für Eingang 2 (I2) überwacht, bevor die Schütze eingeschaltet werden. Hierfür wird ein CROUT-Befehl (Configurable Redundant Output) verwendet. Das System wird durch den Taster, PB1, zurückgesetzt.

Verdrahtung



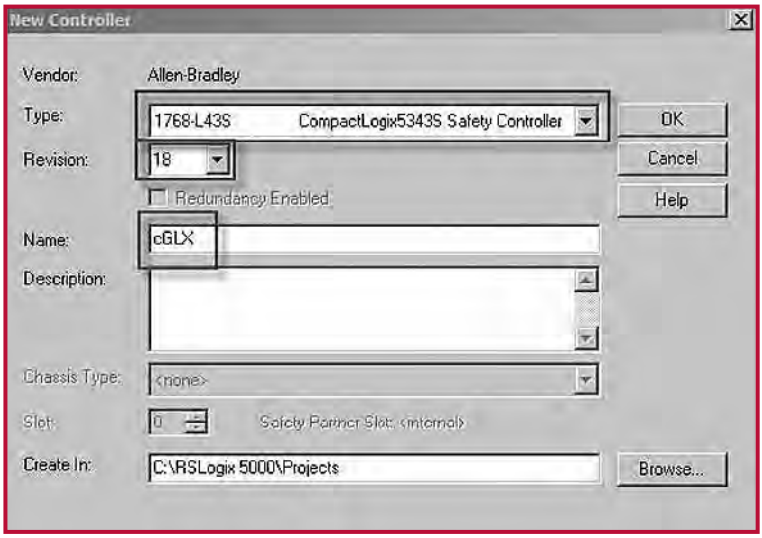
Konfiguration

Die Compact GuardLogix-Steuerung wird mithilfe von RSLogix 5000, Version 18 oder höher, konfiguriert. Sie müssen ein neues Projekt erstellen und die E/A-Module hinzufügen. Anschließend konfigurieren Sie die E/A-Module für die richtigen Eingangs- und Ausgangstypen. Die einzelnen Schritte sind jedoch in diesem Dokument nicht näher beschrieben. Es wird davon ausgegangen, dass der Anwender mit der RSLogix-Programmierumgebung vertraut ist.

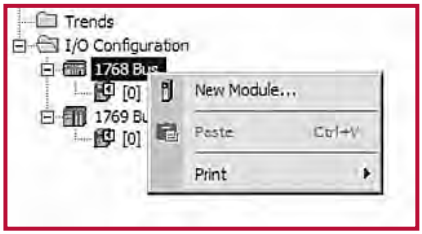
Konfigurieren der Steuerung und Hinzufügen der E/A-Module

Gehen Sie wie folgt vor:

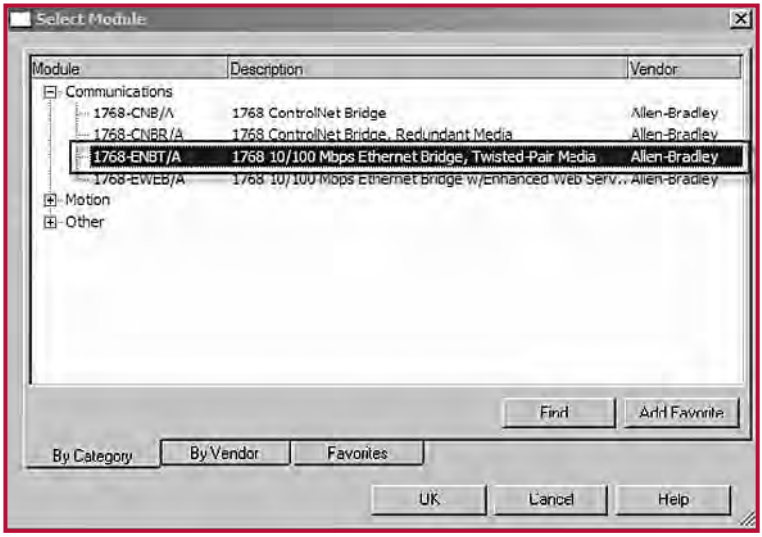
1. Erstellen Sie in der Software RSLogix 5000 ein neues Projekt.



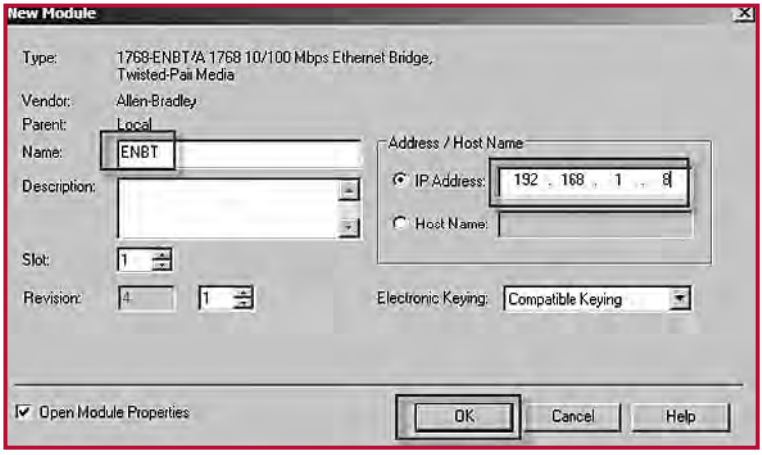
2. Fügen Sie im Controller Organizer (Steuerungsorganisator) dem 1768-Bus das 1768-ENBT-Modul hinzu.



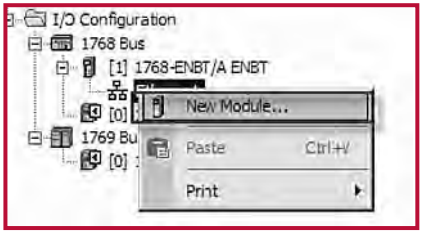
3. Wählen Sie das 1768-ENBT-Modul aus und klicken Sie auf OK.



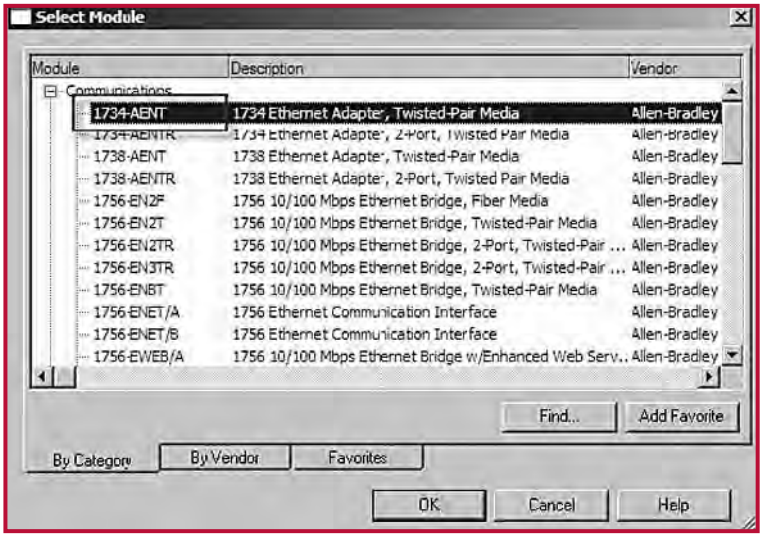
4. Benennen Sie das Modul, geben Sie seine IP-Adresse ein und klicken Sie auf OK. Für dieses Anwendungsbeispiel wurde die Adresse 192.168.1.8 verwendet. Ihre Adresse unterscheidet sich eventuell von dieser Adresse.



5. Fügen Sie den 1734-AENT-Adapter hinzu, indem Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf das 1768-ENBT-Modul klicken und „New Module“ (Neues Modul) auswählen.

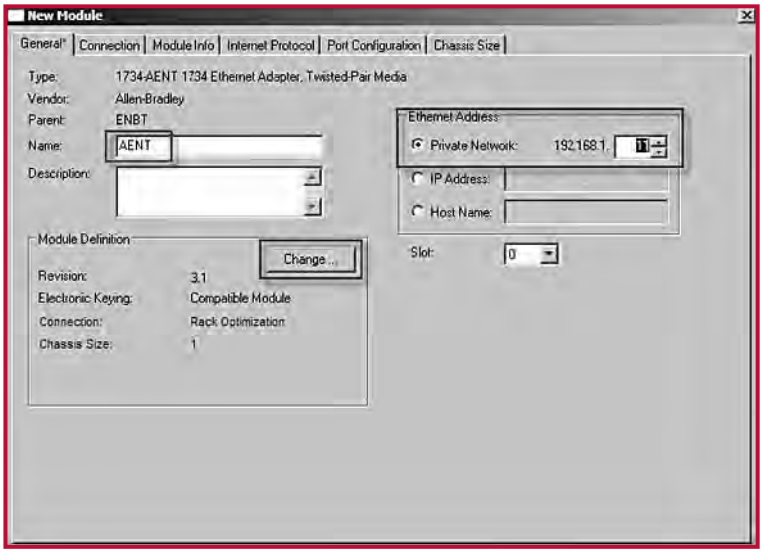


6. Wählen Sie den 1734-AENT-Adapter aus und klicken Sie auf OK.


Select Module
Module
Description
Vendor
Communications
1734-AENT 1734 Ethernet Adapter, Twisted-Pair Media Allen-Bradley
1734-AENTR 1734 Ethernet Adapter, 2-Port, Twisted Pair Media Allen-Bradley
1738-AENT 1738 Ethernet Adapter, Twisted-Pair Media Allen-Bradley
1738-AENTR 1738 Ethernet Adapter, 2-Port, Twisted Pair Media Allen-Bradley
1756-EN2F 1756 10/100 Mbps Ethernet Bridge, Fiber Media Allen-Bradley
1756-EN2T 1756 10/100 Mbps Ethernet Bridge, Twisted-Pair Media Allen-Bradley
1756-EN2TR 1756 10/100 Mbps Ethernet Bridge, 2-Port, Twisted-Pair ... Allen-Bradley
1756-EN3TR 1756 10/100 Mbps Ethernet Bridge, 2-Port, Twisted-Pair ... Allen-Bradley
1756-ENBT 1756 10/100 Mbps Ethernet Bridge, Twisted-Pair Media Allen-Bradley
1756-ENET/A 1756 Ethernet Communication Interface Allen-Bradley
1756-ENET/B 1756 Ethernet Communication Interface Allen-Bradley
1756-EWEB/A 1756 10/100 Mbps Ethernet Bridge w/Enhanced Web Serv... Allen-Bradley
Find...
Add Favorite
By Category
By Vendor
Favorites
OK
Cancel
Help

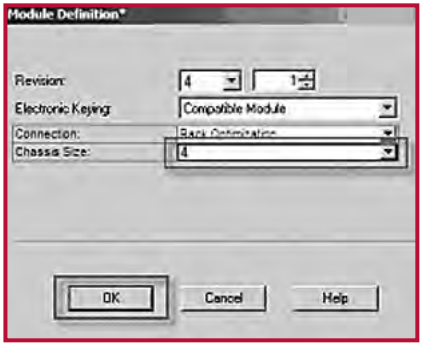
7. Benennen Sie das Modul, geben Sie seine IP-Adresse ein und klicken Sie auf OK. Für dieses Anwendungsbeispiel wurde die Adresse 192.168.1.11 verwendet. Ihre Adresse unterscheidet sich eventuell von dieser Adresse.

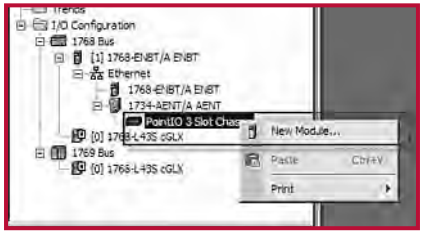
8. Klicken Sie auf „Change“ (Ändern).



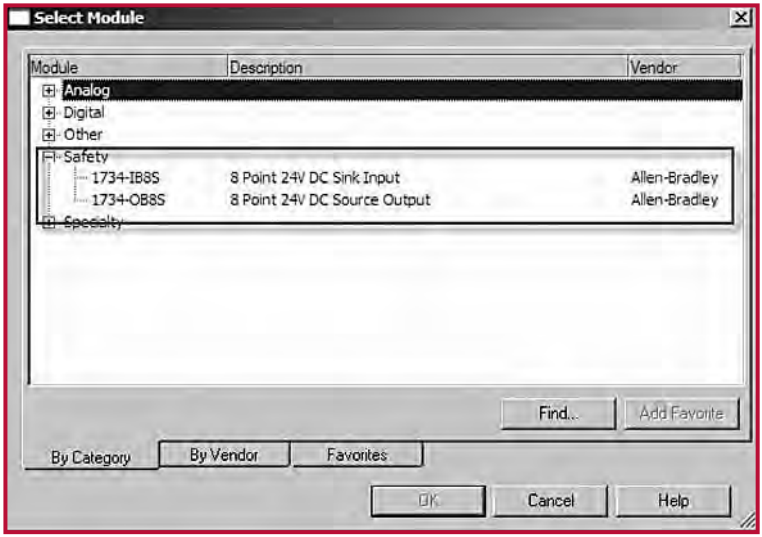
9. Legen Sie im Feld „Chassis Size“ (Chassisgröße) den Wert 4 für den 1734-AENT-Adapter fest und klicken Sie auf OK. Die Chassisgröße entspricht der Anzahl der Module, die in das Chassis eingesetzt werden. Es wird davon ausgegangen, dass sich der 1734-AENT-Adapter in Steckplatz 0 befindet, sodass Chassisgröße 4 für zwei Eingangsmodule und ein Ausgangsmodul gilt.

10. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf den 1734-AENT-Adapter und wählen Sie „New Module“ (Neues Modul) aus.

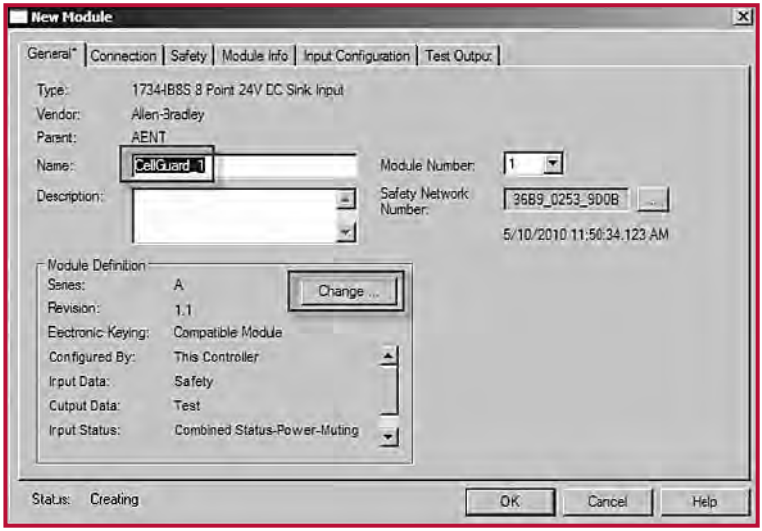




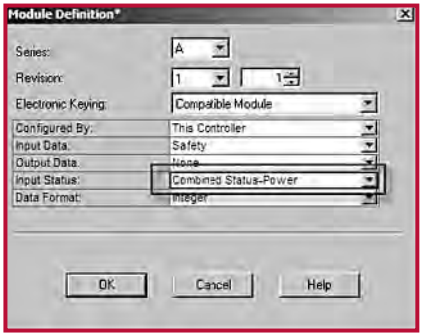
11. Erweitern Sie den Knoten „Safety“ (Sicherheit), wählen Sie das 1734-IB8S-Modul aus und klicken Sie auf OK.



12. Geben Sie im Dialogfeld „New Module“ (Neues Modul) für das Gerät den Namen „CellGuard_1“ ein und klicken Sie auf „Change“ (Ändern).



13. Wenn das Dialogfeld „Module Definition“ (Moduldefinition) geöffnet wird, ändern Sie im Feld „Input Status“ (Eingangsstatus) den Wert in „Combined Status-Power“ (Kombiniert Status-Leistung) und klicken Sie auf OK.



14. Schließen Sie das Dialogfeld „Module Properties“ (Moduleigenschaften) und klicken Sie auf OK.

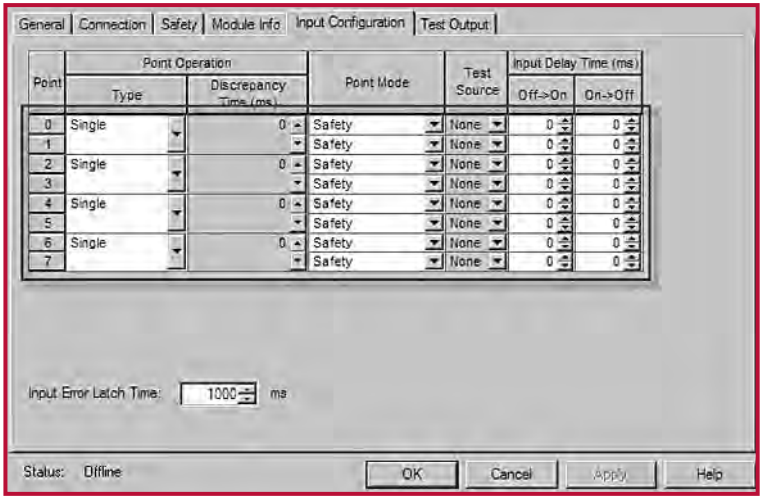
15. Wiederholen Sie die Schritte 10 bis 14, um ein zweites 1734-IB8S-Sicherheitseingangsmodul und ein 1734-OB8S-Sicherheitsausgangsmodul hinzuzufügen.

Konfigurieren Sie die E/A-Module

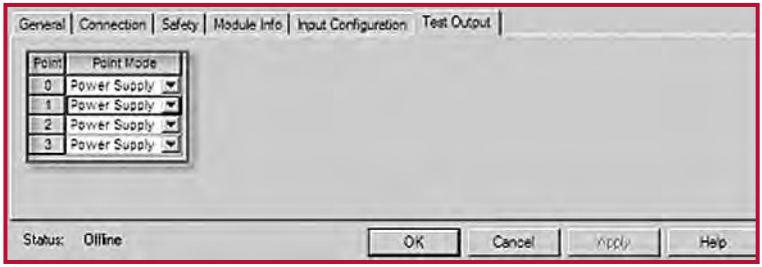
Gehen Sie wie folgt vor, um die POINT Guard I/O-Module zu konfigurieren.

1. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf ein 1734-IB8S-Modul und wählen Sie „Properties“ (Eigenschaften) aus.

2. Klicken Sie auf „Input Configuration“ (Eingangskonfiguration) und konfigurieren Sie das Modul wie angegeben.



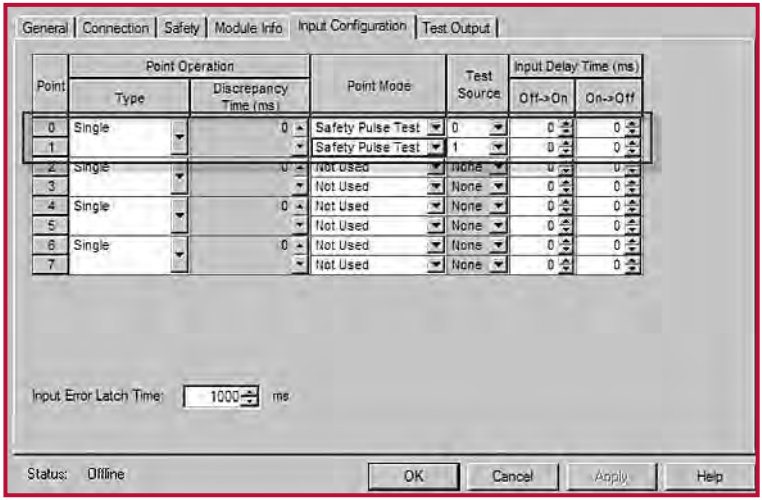
3. Klicken Sie auf „Test Output“ (Ausgang testen) und konfigurieren Sie das Modul wie angegeben.



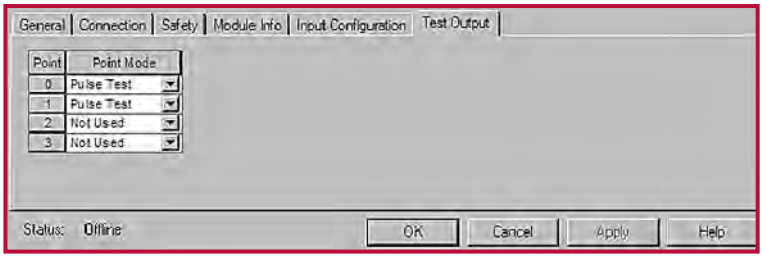
4. Klicken Sie auf OK.

5. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf das zweite 1734-IB8S-Modul und wählen Sie „Properties“ (Eigenschaften) aus.

6. Klicken Sie auf „Input Configuration“ (Eingangskonfiguration) und konfigurieren Sie das Modul wie angegeben.



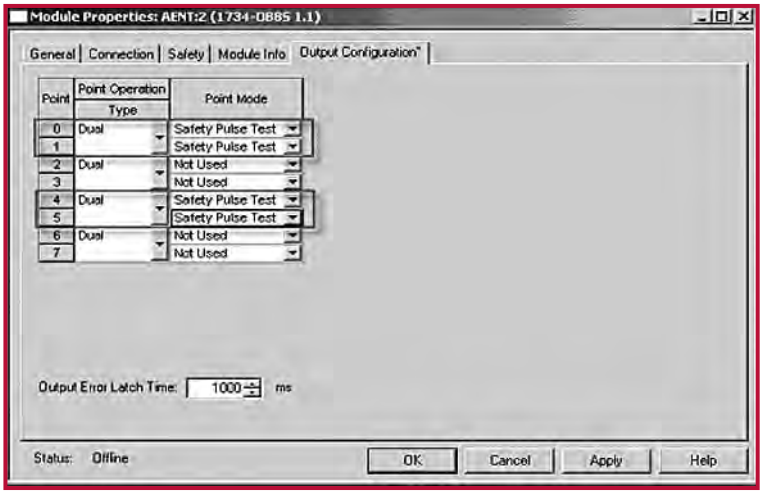
7. Klicken Sie auf „Test Output“ (Ausgang testen) und konfigurieren Sie das Modul wie angegeben.



8. Klicken Sie auf OK.

9. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf das 1734-OB8S-Modul und wählen Sie „Properties“ (Eigenschaften) aus.

10. Klicken Sie auf „Output Configuration“ (Ausgangskonfiguration) und konfigurieren Sie das Modul wie angegeben.

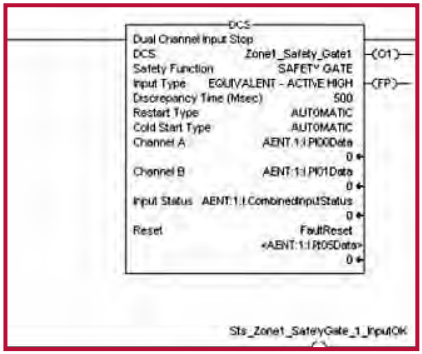


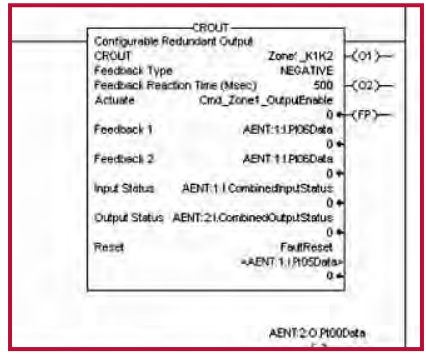
11. Klicken Sie auf OK.

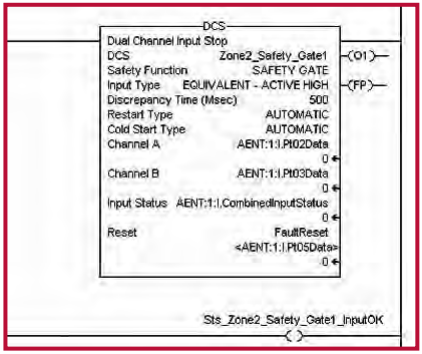
Programmierung

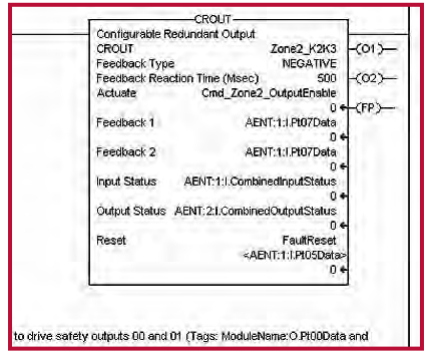
Der Befehl DCS (Dual Channel Input Stop) überwacht Sicherheitsgeräte mit zwei Eingängen, deren Hauptfunktion das sichere Ausschalten einer Maschine ist, z. B. Not-Halt-Geräte, Lichtgitter oder Schutztüren. Dieser Befehl kann Ausgang 1 nur einschalten, wenn beide Sicherheitseingänge, Kanal A und Kanal B, aktiv sind (wie durch den Parameter „Input Type“ (Eingangstyp) festgelegt) und die richtigen Rückstellaktionen ausgeführt werden. Der DCS-Befehl überwacht Kanäle mit zwei Eingängen auf Konsistenz (Äquivalent – High-aktiv). Darüber hinaus erkennt und isoliert er Fehler, wenn eine Inkonsistenz festgestellt wird, die länger andauert als die konfiguriere Diskrepanzzeit (ms). Der CROUT-Befehl (Configurable Redundant Output) steuert und überwacht redundante Ausgänge. Die Reaktionszeit für das Ausgangsfeedback ist konfigurierbar. Der Befehl unterstützt positive und negative Feedbacksignale.

Die Sicherheitsanwendersoftware in der Sicherheitsausgangsroutine hindert Ausgänge vor einem erneuten Start, wenn der Eingangskanal automatisch zurückgesetzt wird. Auf diese Weise steht der Schaltkreisrückstellung eine Antisprung-Funktionalität zur Verfügung.

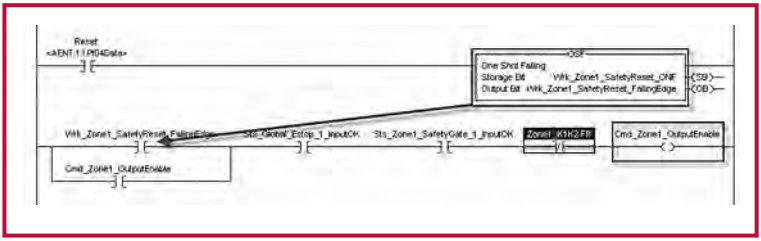








Rückstellung der abfallenden Signalkante
EN ISO 13849-1 gibt an, dass Befehlsrücksetzfunktionen an der abfallenden Signalkante auftreten müssen. Um diese Anforderung zu erfüllen, fügen Sie dem Rückstellcode wie unten dargestellt einen „One Shot Falling"-Befehl (Fallender Einzelimpuls) hinzu.



Leistungsdaten

Bei richtiger Konfiguration kann jede Sicherheitsfunktion die Sicherheitsklassifizierung PLe, KAT 4 gemäß EN ISO 13849.1 2008 erzielen.

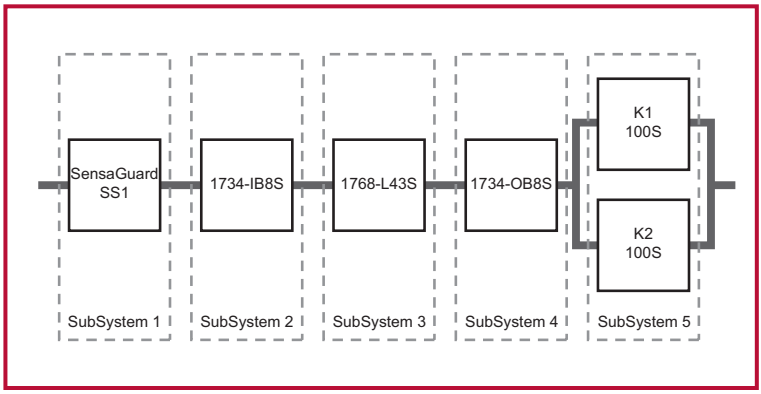
Die Berechnungen basieren auf einer Einsatzzeit von 360 Tagen pro Jahr und 16 Stunden pro Tag, wobei die Schutztür einmal pro Stunde (also insgesamt 5760 Mal pro Jahr) ausgelöst wird. Die globale Not-Halt-Funktion wird einmal pro Monat getestet.

Safety Gate 1	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Estop 1	
PLr	d
PL	e
PFH [1/h]	5E-8

Safety Gate 2	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Jede Schutztürfunktion kann wie folgt dargestellt werden.



SB Interlock Switch: SensaGuard	
PL	e
PFH [1/h]	1.12E-9
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

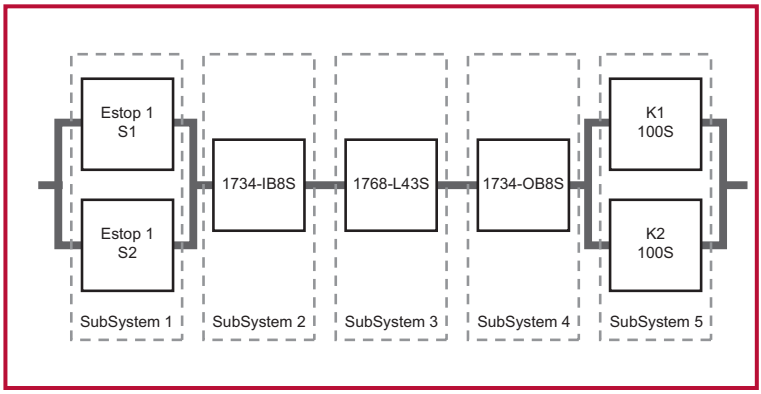
SB Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Die Not-Halt-Funktion kann wie folgt dargestellt werden.



SB Estop 1	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

SB Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Dieses Beispiel, seine SISTEMA-Berechnungsdatei und die RSLogix 5000-Anwendersoftware können von der folgenden Webseite heruntergeladen werden:

www.discoverrockwellautomation.com

Weitere Informationen zu den in diesem Beispiel verwendeten Produkten finden Sie in der Rockwell Automation-Literaturbibliothek, indem Sie nach den unten hervorgehobenen Publikationsnummern suchen. Allgemeine Produktübersichten finden Sie alternativ auf der Webseite www.ab.com.

Die URL der Literaturbibliothek lautet wie folgt: **www.theautomationbookstore.com**

Literatur	**Beschreibung**
Compact GuardLogix-Steuerungen Benutzerhandbuch. Publikation: **1768-UM002**	Enthält Informationen zur Konfiguration, Bedienung und Wartung von Compact GuardLogix-Steuerungen
POINT Guard I/O-Sicherheitsmodule Installations- und Benutzerhandbuch. Publikation: **1734-UM013**	Enthält Informationen zum Installieren, Konfigurieren und Bedienen von POINT Guard I/O-Modulen
Steuerungssysteme GuardLogix Sicherheitsreferenzhandbuch. Publikation: **1756-RM093**	Enthält ausführliche Anforderungen zum Erzielen und Warten von Sicherheits-klassifizierungen mit dem GuardLogix-Steuerungssystem
Befehlssatz für GuardLogix-Sicherheitsanwendungen – Referenzhandbuch. Publikation: **1756-RM095**	Enthält ausführliche Informationen zum Befehlsatz für die GuardLogix-Sicherheits-anwendungen
Safety Accelerator Toolkit for GuardLogix Systems, Quick Start Guide. Publikation: **IASIMP-QS005**	Enthält schrittweise Anleitungen zur Verwendung der Entwicklungs-, Programmier- und Diagnosetools im Safety Accelerator Toolkit
Katalog zu Sicherheitsprodukten Publikation: **S117-CA001A**	Eine umfassende Publikation zu Sicher-heitsprodukten, Anwendungsbeispielen und mit vielen nützlichen Informationen

Rockwell Automation hat eine Reihe ähnlicher Beispiele entwickelt, die über die Literatur-bibliothek heruntergeladen werden können. Rufen Sie die Literaturbibliothek auf und geben Sie in das Suchfeld „SAFETY-AT“ ein (wählen Sie im Dropdown-Menü die Option „Publication Number“ aus.

SISTEMA-Berechnungen und RSLogix 5000-Anwendersoftware stehen für einige der Anwendungen bereit und können von der folgenden Webseite heruntergeladen werden:

www.discoverrockwellautomation.com

MTTFd für jeden Kanal in Jahren	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (1/h) und entsprechender Performance Level (PL)													
	Kat. B	PL	Kat. 1	PL	Kat. 2	PL	Kat. 2	PL	Kat. 3	PL	Kat. 3	PL	Kat. 4	PL
	$DC_{Durchschn}$ = keine		$DC_{Durchschn}$ = keine		$DC_{Durchschn}$ = niedrig		$DC_{Durchschn}$ = mittel		$DC_{Durchschn}$ = niedrig		$DC_{Durchschn}$ = mittel		$DC_{Durchschn}$ = hoch	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

MTTFd für jeden Kanal in Jahren	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (1/h) und entsprechender Performance Level (PL)													
	Kat. B	PL	Kat. 1	PL	Kat. 2	PL	Kat. 2	PL	Kat. 3	PL	Kat. 3	PL	Kat. 4	PL
	$DC_{Durchschn}$ = keine		$DC_{Durchschn}$ = keine		$DC_{Durchschn}$ = niedrig		$DC_{Durchschn}$ = mittel		$DC_{Durchschn}$ = niedrig		$DC_{Durchschn}$ = mittel		$DC_{Durchschn}$ = hoch	
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation, Düsselberger Straße 15, D-42781 Haan, Tel.: +49 (0)2104 960 0, Fax: +49 (0)2104 960 121
Schweiz: Rockwell Automation, Buchserstrasse 7, CH-5001 Aarau, Tel.: +41(62) 889 77 77, Fax: +41(62) 889 77 11
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel.: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation: SAFEBK-RM002B-DE-P – März 2011
Ersetzt Publikation: SAFEBK-RM002A-DE-P

© 2011 Rockwell Automation, Inc. Alle Rechte vorbehalten.